Milestone Systems

XProtect® Professional 2014

Administrator's Manual

milestone

The Open Platform Company

Contents

BEFORE YOU START 10

ABOUT MINIMUM SYSTEM REQUIREMENTS 10

ABOUT ADMINISTRATOR RIGHTS 10

ABOUT IMPORTANT PORT NUMBERS 10

ABOUT DAYLIGHT SAVING TIME 11

ABOUT TIME SERVERS 11

ABOUT VIRUS SCANNING 12

SYSTEM OVERVIEW 13

SYSTEM OVERVIEW 13

CLIENTS 15

XProtect Smart Client 15

Milestone Mobile client 17

XProtect Web Client 19

RECORDING SERVER MANAGER 20

XPROTECT DOWNLOAD MANAGER 21

LICENSES 24

About licenses 24

About seeing license information 25

About replacing cameras 25

INSTALL AND UPGRADE 27

INSTALL YOUR SYSTEM SOFTWARE 27

INSTALL SILENTLY 27

INSTALL VIDEO DEVICE DRIVERS 29

UPGRADE 29
About upgrading 29
About updates 29
Upgrading from one product version to another product version 30
Upgrading from one current XProtect Professional VMS product to another current XProtect Professional VMS product 31
ABOUT REMOVING SYSTEM COMPONENTS 31
FIRST TIME USE 33
GET YOUR SYSTEM UP AND RUNNING 33
BEST PRACTICES 34
About protecting recording databases from corruption 34
About saving changes to the configuration 35
About using the built-in help 36
About restarting services 37
Monitor storage space usage 37
View video from cameras in Management Application 38
GETTING STARTED 39
ABOUT THE GETTING STARTED PAGE 39
AUTOMATIC CONFIGURATION WIZARD 39
Automatic configuration wizard: First page 39
Automatic configuration wizard: Scanning options 39
Automatic configuration wizard: Select hardware manufacturers to scan for 39
Automatic configuration wizard: Scanning for hardware devices 40
Automatic configuration wizard: Continue after scan 40
ADD HARDWARE WIZARD 40
Express 41
Manual 42
CONFIGURE STORAGE WIZARD 44

Configure storage: Video settings and preview 44
Configure storage: Online schedule 45
Configure storage: Live and recording settings (motion JPEG cameras) 46
Configure storage: Live and recording settings (MPEG cameras) 47
Configure storage: Drive selection 49
Configure storage: Recording and archiving settings 51

ADJUST MOTION DETECTION WIZARD 52
Adjust motion detection: Exclude regions 53
Adjust motion detection: Motion detection 53

MANAGE USER ACCESS WIZARD 55
Manage user access: Basic and Windows users 55
Manage user access: Access summary 56

ADVANCED CONFIGURATION 57

HARDWARE DEVICES 57
About hardware devices 57
About microphones 57
About speakers 57
About recording audio 57
About dedicated input/output devices 58
Show or hide microphones or speakers 58
Configure hardware devices 59
Delete hardware devices 59
About replacing hardware devices 59
About the Replace Hardware Device wizard 60
Speaker properties 62
Hardware properties 62

CAMERAS AND STORAGE INFORMATION 64
About video and recording configuration 64
About database resizing 65

About motion detection 65
About motion detection and PTZ cameras 67
Configure camera-specific schedules 67
Configure when cameras should do what 69
Configure motion detection 69
Disable or delete cameras 69
Move PTZ type 1 and 3 to required positions 70
Recording and storage properties 71
Camera properties 86

MICROPHONES 106
About microphones 106
Configure microphones or speakers 106
Show or hide microphones or speakers 107
Microphone (properties) 107

EVENTS AND OUTPUT 108
About input and output 108
About events and output 108
Overview of events and output 108
Add an analytics event 110
Add a hardware input event 110
Add a hardware output 111
Add a manual event 112
Add a generic event 112
Add a timer event 113
Configure hardware output on event 113
Configure general event handling 114
Generate alarms based on analytics events 114
Test a generic event 114
General event properties 116
Events and output properties 117

SCHEDULING AND ARCHIVING 125
About scheduling 125
About archiving 126
Configure general scheduling and archiving 131
General scheduling properties 131
Camera-specific scheduling properties 134
MATRIX 136
About Matrix video sharing 136
About Matrix-recipients 136
Configure Matrix 137
Matrix properties 137
LOGS 139
About logs 139
Configure system, event and audit logging 142
Log properties 142
NOTIFICATIONS 144
About notifications 144
Email 144
SMS 147
Scheduling 149
CENTRAL 150
About Central 150
Enable XProtect Central 150
Central properties 150
ACCESS CONTROL 151
About access control integration 151
Wizard for access control system integration 151
Access control properties 153
SERVER ACCESS 158

About server access 158
About registered services 158
Configure server access 159
Server access properties 159

MASTER/SLAVE 161
About master and slave 161
Configure master and slave servers 161
Master/slave properties 161

USERS 163
About users 163
Add basic users 163
Add Windows users 163
Add user groups 164
Configure user and group rights 165
User properties 165

SERVICES 169
About services 169
Start and stop services 170

SERVERS 170
Mobile server 170

ALARMS 181
About alarms 181
About maps 182
Add an alarm 183
Add a time profile (for alarms) 183
Alarms properties 184

MIP PLUG-INS 187
About MIP plug-ins 187

SETTINGS 188

ABOUT AUTOMATIC DEVICE DISCOVERY 188

DISABLE INFORMATION COLLECTION 188

CHANGE DEFAULT FILE PATHS 188

OPTIONS 189

General 189

User Interface 190

Default File Paths 191

Analytics Event Settings 191

Event Server Settings 192

SYSTEM MAINTENANCE 194

BACK UP AND RESTORE CONFIGURATION 194

About back up and restore of configuration 194

Back up system configuration 194

Restore system configuration 195

Back up and restore alarm and map configuration 195

Export and import management application configuration 198

Import changes to configuration 199

Restore system configuration from a restore point 200

GLOSSARY OF TERMS 201

INDEX 209

Copyright, trademarks and disclaimer

Copyright

© 2014 Milestone Systems A/S.

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file **3rd_party_software_terms_and_conditions.txt** located in your Milestone surveillance system installation folder.

Before you start

About minimum system requirements

Important: Your system no longer supports Microsoft® Windows® 2003 (however, you can still run/access clients from computers with Windows 2003).

Important: Your system no longer supports Microsoft® Windows® 32-bit OS (however, you can still run/access XProtect Web Client and XProtect Smart Client from computers with Windows 32-bit OS).

For information about the **minimum** system requirements to the various components of your system, go to www.milestonesys.com/systemrequirements.

About administrator rights

When you install the surveillance system, it is important that you have administrator rights on the computer that should run the system. If you only have standard user rights, you cannot configure the surveillance system.

About important port numbers

Your system uses particular ports when communicating with other computers, cameras, and so on. Make sure that the following ports are open for data traffic on your network when you use your system:

Name	Description
Port 20 and 21 (inbound and outbound)	Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.
Port 25 (inbound and outbound)	Used for SMTP traffic. Simple Mail Transfer Protocol (SMTP) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.
Port 80 (inbound and outbound)	Used for HTTP traffic between the surveillance server, cameras, and XProtect Smart Client, and the default communication port for the surveillance system's Image Server service.
Port 554 (inbound and outbound)	Used for RSTP traffic in connection with H.264 video streaming.
Port 1024 (outbound only)	Used for HTTP traffic between cameras and the surveillance server.
Port 1234 (inbound and outbound)	Used for event handling.

Name	Description
Port 1237 (inbound and outbound)	Used for communication with the XProtect Central add-on product.
Port 8081 and 8082	Used for communication with the Mobile service.
Port 22331	Used for communication with the Event Server service.

Your organization may also have selected to use any other port numbers, for example if you have changed the server access (on page 159) port from its default port number (80) to another port number.

About daylight saving time

Daylight saving time (DST) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. The use of DST varies between countries/regions.

When you work with a surveillance system, which is inherently time-sensitive, it is important that you know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day has 23 hours. In that case, there is no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day has 25 hours. In that case, you reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, your system forcefully archives the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour is not viewable directly from clients. However, the data is recorded and safe, and it can be browsed using the XProtect Smart Client by opening the archived database directly.

About time servers

Once your system receives images, they are instantly time-stamped. Since cameras are separate units which may have separate timing devices, camera time and your system time may not correspond fully. This may occasionally lead to confusion. If your cameras support timestamps, Milestone recommends that you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about how to configure a time server, search www.microsoft.com for **time server**, **time service**, or similar.

About virus scanning

As is the case with any other database software, if an antivirus program is installed on a computer running XProtect® software, it is important that you exclude specific file types and locations, as well as certain network traffic. Without implementing these exceptions, virus scanning uses a considerable amount of system resources. On top of that, the scanning process can temporarily lock files which likely results in a disruption in the recording process or even database corruption.

When you need to perform virus scanning, do not scan Recording Server directories containing recording databases (by default c:\mediadatabase\, as well as all folders under that location). Avoid also to perform virus scanning on archive storage directories. In older versions of the software, the databases are by default located in the installation folder, each being a subfolder with the MAC address of the device recorded.

Create the following additional exclusions:

- File types: .blk, .idx, .pic, .pqz, .sts, .ts
- C:\Program Files\Milestone or C:\Program Files (x86)\Milestone and all subdirectories.
- Exclude network scanning on TCP ports:

Product	TCP ports
XProtect® Corporate, XProtect® Expert	80, 8080, 7563, 25, 21, 9993
XProtect® Enterprise, XProtect® Professional, XProtect® Express, XProtect® Essential, XProtect® Basis+	80, 25, 21, 1234, 1237, 22331
XProtect® Mobile	8081
XProtect® Transact	9001

or

- Exclude network scanning of the following processes:

Product	Processes
XProtect Corporate, XProtect Expert	*VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe*
XProtect Enterprise, XProtect Professional, XProtect Express, XProtect Essential, XProtect Basis+	*RecordingServer.exe, ImageServer.exe, ManagementApplication.exe, ImageImportService.exe, RecordingServerManager.exe, VideoOS.ServiceControl.Service.exe, VideoOS.Event.Server.exe*
XProtect Mobile	*VideoOS.MobileServer.Service.exe*
XProtect Transact	*VideoOS.Transact.TransactService.exe*

Organizations may have strict guidelines regarding virus scanning, however it is important that the above locations and files are excluded from virus scanning.

System overview

System overview

Your surveillance system is the right product for small to mid-sized installations that need robust single-server surveillance software with the full functionality of advanced management, flexible scheduling, fast searching and analysis. Your system supports up to 64 cameras simultaneously with the widest choice of network video and computer hardware equipment.

Your system consists of a number of components, each targeted at specific tasks and user types:

Name	Description
Management Application	The main application for configuring the surveillance system server, for example when you add new cameras, set up users or change configuration on the system.
Recording Server service	A vital part of the surveillance system. The Recording Server service runs to ensure that devices transfer video streams to your system. The Recording Server service installs automatically and runs in the background on the surveillance system server. You manage the service through the Management Application.
Event Server service	Handles configuration of alarms and maps from all servers within the surveillance system installations, including Master/slave setups, throughout your organization. This enables monitoring and instant overview of alarms and possible technical problems within your systems. The event server is automatically installed on the surveillance system server where it runs in the background.
Microsoft® SQL Server Express Database	The surveillance system's alarm data is stored in a SQL Server Express database. The SQL database is a lightweight, yet powerful, version of a full SQL server which is automatically installed on, and runs in the background of, your surveillance system server.
Image Server service	Handles access to the surveillance system for users logging in with clients. The Image Server service is automatically installed and runs in the background on the surveillance system server. You can manage the service through the Management Application.
XProtect® Download Manager	Manages the system-related features your organization's users can access from a targeted welcome page on the surveillance system server.
XProtect® Smart Client	Designed for Milestone XProtect surveillance systems, XProtect Smart Client is a client application for the daily operations of security installations. Its streamlined interface makes it easy to monitor installations of all sizes, manage security incidents and access and export live and recorded video. Milestone recommends that you always use the latest version of XProtect Smart Client to best use new features and functions included in your surveillance system.

Name	Description
Milestone® Mobile client	A free application designed by Milestone that allows you to view video from your system from almost anywhere on your smartphone or tablet. You can also control outputs, such as opening and closing doors and switching lights on or off, allowing you to gain control and dynamically respond to incidents in the system.
XProtect® Web Client	A simplified web-based client application for XProtect surveillance systems for viewing, playing back and sharing video from most operating systems and web browsers. With no need to install additional software, you can monitor your system from any computer or Internet connection.

Clients

Clients are applications used for viewing live and recorded video from the hardware devices set up in the Management Application.

Your system supports three different clients:

- XProtect Smart Client
- Milestone Mobile client
- XProtect Web Client

XProtect Smart Client

About XProtect Smart Client

Designed for Milestone XProtect® IP video management software, the XProtect Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with XProtect Smart Client which gives users access to live and recorded video, instant control of cameras and connected security devices, and an overview of recordings. Available in multiple local languages, XProtect Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.

The interface allows you to tailor your viewing experience to specific working environments by selecting a light or dark theme, depending on room lighting or brightness of the video. It also features work-optimized tabs and an integrated video timeline for easy surveillance operation. Using the Milestone Integration Platform, users can integrate various types of security and business systems and video analytics applications, which you manage through XProtect Smart Client.

XProtect Smart Client must be installed on users' computers. Surveillance system administrators manage clients' access to the surveillance system through the Management Application. Recordings viewed by clients are provided by your XProtect system's Image Server service. The service runs in the background on the surveillance system server. Separate hardware is not required.

To download XProtect Smart Client, you must connect to the surveillance system server which presents you with a welcome page that lists available clients and language versions. System administrators can use XProtect Download Manager to control what clients and language versions should be available to users on the welcome page of the XProtect Download Manager.

Install XProtect Smart Client

You must install XProtect Smart Client on your computer before you can use it. You download XProtect Smart Client from the surveillance system server and install it on your computer or install directly from a DVD.

Install from the management server

Before you begin, verify that your computer meets the XProtect Smart Client's minimum system requirements.

1. Open an Internet Explorer browser (version 6.0 or later) and connect to the management server using the URL or IP address of that server.
2. On the Welcome page, click **Language** and select the language you want to use.
3. The XProtect Smart Client **setup** wizard starts. In the wizard, follow the installation instructions.

The wizard suggests an installation path. Normally, you can use the suggested installation path. However, if you have previously used add-on products, such as XProtect LPR, this path might not be valid anymore.

Install silently

A surveillance system administrator can deploy the system or XProtect Smart Client to users' computers by using tools such as Microsoft Systems Management Server (SMS). With this tool, you can build up databases of hardware and software on local networks. You can then use the databases for distributing and installing software applications over local networks.

To install silently:

1. Locate the XProtect Smart Client .exe file **MilestoneXProtectSmart Client_x64.exe**. Find the file in a subfolder under the folder **httpdocs**. The **httpdocs** folder is located under the folder in which your Milestone surveillance software is installed.

   The path is typically (if you are using an English language version of the XProtect Smart Client):
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\XProtect Smart Client Installer\[version number] [bit-version]\All Languages\en-US

   For example:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\XProtect Smart Client Installer\2014 (64-bit)\All Languages\en-US

2. Run a silent installation using one of the following two options:

   a) Run with default parameter settings:

To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and execute following command:

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --quiet

  Your system:

  MilestoneXProtectProfessionalVMS_installer_x64.exe --quiet

This performs a quiet installation of XProtect Smart Client or your system using default values for parameters such as target directory and so on. To change the default settings, see the following:

a) Customize default parameters using an XML argument file as input:

In order to customize the default installation settings, you must provide an XML file with modified values as input. In order to generate the XML file with default values, open a command prompt in the directory where the installation program is located and execute following command:

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --generateargsfile=[full path]args.xml

- Your system:

  MilestoneXProtectProfessionalVMS_installer_x64.exe --generateargsfile=[full path]args.xml

Open the generated args.xml file in a text editor and perform any changes needed. Then execute the following command in the same directory to run a modified version of the silent installation.

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --arguments=[full path]args.xml --quiet

- Your system:

  MilestoneXProtectProfessionalVMS_installer_x64.exe --arguments= [full path]args.xml --quiet

Milestone Mobile client

About Milestone Mobile client

Milestone® Mobile client is a mobile surveillance solution closely integrated with the rest of your XProtect system. It runs on your Android tablet or smartphone or your Apple® tablet, smartphone or portable music player and gives you access to cameras, views and other functionality set up in the Management Application. Use the Milestone Mobile client to view and play back live and recorded video from one or multiple cameras, control pan-tilt-zoom (PTZ) cameras, trigger output and events and use the Video push functionality to send video from your device to your XProtect system.

If you want to use Milestone Mobile client with your system, you must add a Mobile server to establish the connection between the Milestone Mobile client and your system. Once the Mobile server is set up, download the Milestone Mobile client for free from Google Play or App Store to start using Milestone Mobile.

Install Milestone Mobile client

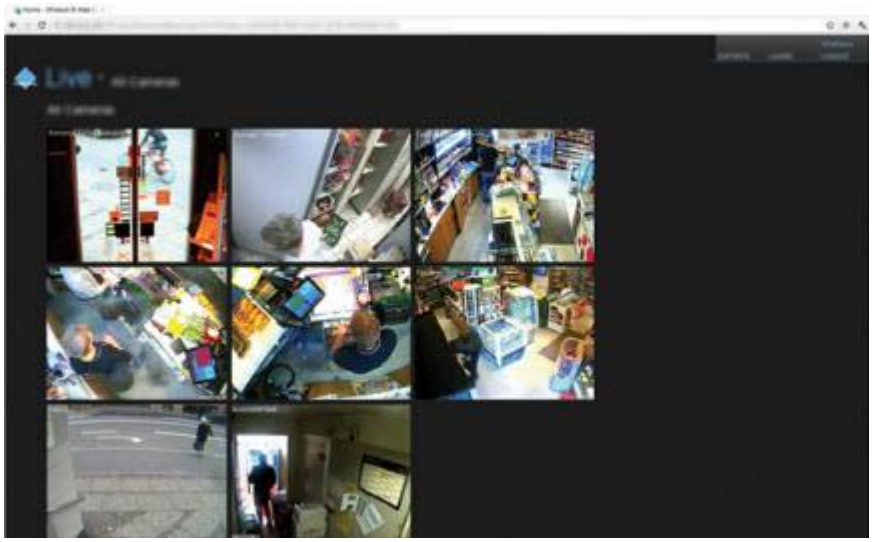
1. Access Google Play or App Store℠ on your device.
2. Search for and download the application Milestone Mobile.
3. Once the download of the application is completed, the Milestone Mobile client is ready for use on your mobile device.

For detailed information about how to set up your Milestone Mobile client, visit the Milestone website at www.milestonesys.com.

XProtect Web Client

About XProtect Web Client

XProtect Web Client is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used surveillance functions, such as viewing live video, play back recorded video, print and export evidence. Access to features depends on individual user rights which are set up in the Management Application.



To enable access to the XProtect Web Client, you must install a Mobile server to establish the connection between the XProtect Web Client and your system. The XProtect Web Client itself does not require any installation itself and works with most Internet browsers. Once you have set up the Mobile server, you can monitor your XProtect system anywhere from any computer or tablet with Internet access (provided you know the right external/Internet address, user name and password).

Access XProtect Web Client

If you have a Milestone Mobile server installed on your computer, you can use the XProtect® Web Client to access your cameras and views. Since you do not need to install XProtect Web Client, you can access it from the local computer on which you installed the Milestone Mobile server or any other computer you want to use for this purpose.

To access the XProtect Web Client:

1. Set up the Milestone Mobile server in the Management Application.
2. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari) or click **Open XProtect Web Client** in the Mobile Server Manager (see "About Mobile Server Manager" on page 178).
3. Type in the IP address (that is, the external address and port of the server on which the Milestone Mobile server is running.

Example: The Milestone Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (default settings of the installer).

In the address bar of your browser, type: http://127.2.3.4:8081 or https://127.2.3.4:8082, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using XProtect Web Client.

4. Add the address as a bookmark in your browser for easy future access to XProtect Web Client. If you use XProtect Web Client on the local computer on which you installed the Milestone Mobile server, you can also use the desktop shortcut created by the installer. Click the shortcut to launch your default browser and open XProtect Web Client.

You must clear the chase of Internet browsers running the XProtect Web Client before you can use a new version of the XProtect Web Client. System administrators must ask their XProtect Web Client users to clear out their browser's cache upon upgrade or force this action remotely (you can do this action only in Internet Explorer in a domain).

Recording Server Manager

The Recording Server service is a vital part of the surveillance system. Video streams are only transferred to your system while the Recording Server service is running. The Recording Server Manager informs you about the state of the Recording Server service. It also lets you manage the service.

In the notification area (the system tray), the Recording Server Manager's icon indicates whether the Recording Server service is running or not.

- A green icon in the notification area indicates that the Recording Server service is running.

- A red icon in the notification area indicates that the Recording Server service has stopped.

By right-clicking the icon, you can open the Management Application, start and stop the Recording Server service, view log files, and view version information.

Monitor System Status

Right-click the notification area's Recording Server icon and select **Show System Status** to get access to the **Status** window.

The **Status** window lets you view the status of the image server(s) and connected cameras. The status of each server/camera is indicated by a color:

- **Green** indicates that the server or camera is running correctly.
- **Gray** indicates that the **camera** (not the server) is not running. Typically, a camera is indicated in gray in the following situations:
  - The camera is not online (as defined in the camera's online period schedule).
  - The Recording Server service has been stopped.
- **Red** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware error. Errors are listed in the Recording Server log file.

Place your mouse pointer over a camera in the status window to view details about the relevant camera. The information appears as a pop-up and updates approximately every 10 seconds.

Name	Description
Resolution	The resolution of the camera.
FPS	The number of frames per second (frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
Frame count	The number of frames received from the camera since the Recording Server service was last started.
Received KB	The number of kilobytes sent the by camera since the Recording Server service was last started.
Offline	Indicates the number of times the camera has been offline due to an error.

XProtect Download Manager

Manage which system-related features your organization's users can access from a targeted welcome page on the surveillance system server through the use of XProtect Download Manager.

- Access XProtect Download Manager from Windows' **Start** menu: Select **All Programs** > **Milestone XProtect Download Manager** > **Download Manager**.

Examples of user-accessible features

- **XProtect Smart Client**. Users connect to the surveillance server through an Internet browser where they are presented with a welcome page. From the welcome page, users can download XProtect Smart Client software and install it on their computers.
- **Various plug-ins**. Downloading such plug-ins can be relevant for users if your organization uses add-on products with the surveillance system.

The welcome page

The welcome page links to downloads of various features. Users can select language from a menu in the top right corner of the welcome page.

To view the welcome page, open an Internet browser (for example, Internet Explorer version 6.0 or later) and connect to the following address:

```
http://[surveillance server IP address or hostname]
```

If you have configured the Image Server service with a port number other than the default port 80 (you configure this as part of the server access properties), users must specify the port number as well, separated from the IP address or hostname by a colon:

```
http://[surveillance server IP address or hostname]:[port number]
```

The content of the welcome page is managed through XProtect Download Manager and can look different in different organizations.

Immediately after you install your system, the welcome page provides access to XProtect Smart Client in all languages. You can also download XProtectSmart Client in 32- or 64-bit if you run a 64-bit operating system and in 32-bit if you run a 32-bit operating system. This initial look of the welcome page is automatically provided through XProtect Download Manager's default configuration.

Default configuration of XProtect Download Manager

XProtect Download Manager has a default configuration. This ensures that your organization's users can access standard features without the surveillance system administrator having to set up anything. The XProtect Download Manager configuration is represented in a tree structure.

Download Manager's tree structure explained:

- The **first level of the tree structure** indicates that you are working with a system.
- The **second level** indicates that this is the default setup.
- The **third level** refers to the languages in which the welcome page is available. In the example, the welcome page is available in a dozen languages (English, Arabic, Danish, Dutch, French, and more).
- The **fourth level** refers to the features that you can make available to users. For example, you could limit these features to XProtect Smart Client.
- The **fifth level** (**5**) refers to particular versions of each feature, for example, version 4.0, 32-bit, and more that you can make available to users.
- The sixth **level** (**6**) refers to the language versions of the features which can be made available to users. For XProtect Smart Client, which is only available with all languages embedded, the only option is **All Languages**.

The fact that only standard features are initially available helps reduce installation time and save space on the server. There is no need to have a feature or language version available on the server if nobody is going to use it. You can make more features and/or languages available if you need to.

Making new features available

When you install new features, these are by default selected in XProtect Download Manager and immediately available to users through the welcome page.

You can always show or hide features on the welcome page by selecting or clearing check boxes in the tree structure. You can change the sequence in which features and languages are displayed on the welcome page by dragging items and dropping them in the relevant position.

Hiding and removing features

You can remove features in several ways:

You can **hide features** from the welcome page by clearing check boxes in XProtect Download Manager's tree structure. If you do this, the features are still installed on the surveillance system server, and by selecting check boxes in the tree structure, you can quickly make the features available again.

You can **remove features** which have previously been made available through XProtect Download Manager. This removes the installation of the features on the surveillance system server. The features disappear from XProtect Download Manager, but installation files for the features are kept in the

surveillance system server's **Installers** or relevant language folder, so you can re-install them later if required. To do so:

1. In XProtect Download Manager, click **Remove features...**
2. In the **Remove Features** window, select the features you want to remove.
3. Click **OK** and then click **Yes**.

Licenses

About licenses

There are different types of licenses available for your XProtect system:

- **Base license**. This license is for the XProtect software. You need this to use your system beyond the initial 30-day trial period.
- **Hardware license**. Every device you add to the software requires a license.
- **Add-on license**. Add-on licenses are licenses for use if you purchase optional add-on products such as XProtect LPR or XProtect <Access Control Module 2014>.

All Milestone licenses related to a fully licenses system are contained in a single file, a .lic file which represents your license for the software (base license) and allows you to add a number of cameras to your system (device licenses). This means that you only need to make sure that you add this file to the system in order for your system to be fully working. In the following, see additional information about base licenses and device licenses. Add-on licenses are separate licenses that you purchase along with the add-on software.

Base license

When you install the system, you can add a license file to the system right away to license your software and use the full version of the system.

If you install the system in **Trial** mode instead, you run on a temporary license which is valid for 30 days. When the 30 days have passed, you must purchase a license for the system in order to keep using the system and access its recordings.

Hardware licenses

When you purchase the system, you also purchase a certain number of licenses for the number of hardware devices, for example video encoders or cameras, that you want to run on the system. One hardware device license enables you to run as many camera, speaker, microphone, input and output devices that the hardware device consists of. It also enables you to run the hardware device multiple times on one site or multiple times on multiple sites. Note that speakers are only supported by some XProtect Professional VMS products*.

Once you have installed the various system components, configured the system, and added cameras as well as additional recording servers for a master/slave setup, your added devices initially run on temporary licenses that you must activate before a certain period of time ends. This is called the grace period. If grace periods expire on one or more of your devices and you have not activated any licenses, recording servers and cameras do not send data to the surveillance system. Milestone recommends that you activate your licenses before you make final adjustments to your system and its devices.

If you add more device channels than you currently have licenses for, you must buy additional licenses before the cameras can send data to your system. If you are short of licenses, you can disable less important cameras to allow new cameras to run instead. To disable or enable a camera, expand **Hardware Devices**. Select the relevant hardware device, right-click the relevant camera, and select **Enable** or **Disable**.

Note that if your system is connected to the Internet, your licenses are automatically activated as you add devices to system. You do not need to specify any user name or password. The system checks every fifteen minutes if the license file corresponds to the number of installed cameras. If you have added cameras within that time frame, the system automatically adds the license for these cameras as well.

For a step-by-step guide of how to license your device channels as well as your system software, see the separate licensing guides for the 2013 and 2014 versions of the XProtect Professional VMS products, available on the Milestone website at www.milestonesys.com.

* XProtect Professional VMS Products cover the following products: XProtect Enterprise, XProtect Professional, XProtect Express, XProtect Essential and XProtect Go.

About seeing license information

You can get an overview of your licenses by expanding **Advanced Configuration** > **Hardware Devices**. This presents you with the **Hardware Device Summary** table.

Name	Description
Hardware Device Name	Hardware devices (typically cameras but could also be dedicated input/output boxes).
License	Licensing status of your hardware devices. The following statuses can be shown: **Licensed**, **[number of] day(s) grace, Trial,** or **Expired**.
Video Channels	Number of available video channels on your hardware devices.
Licensed Channels	Number of video channels on each of your hardware devices for which you have a license.
Speaker Channels	Number of available speaker channels on your hardware devices.
Microphone Channels	Number of available microphone channels on your hardware devices.
Address	http addresses of your hardware devices.
WWW	Links to http addresses of your hardware devices.
Port	Port used by your hardware devices.
Device Driver	Names of device drivers associated with your hardware devices.

Cameras (or dedicated input/output boxes) for which you are missing a license do not send data to the surveillance system. Cameras added after all available licenses are used are unavailable.

About replacing cameras

If you remove a camera from a recording server, you also free a license. You can replace a licensed camera and activate and license a new camera instead. The total number of purchased device channels corresponds to the total number of cameras that can run on the surveillance system simultaneously.

When you replace a camera, you must use the Replace Hardware Device wizard (see "About the Replace Hardware Device wizard" on page 60) to map all relevant databases of cameras, microphones, inputs, outputs, and more. Remember to activate the license once you are finished.

Install and upgrade

Install your system software

Do not install your surveillance software on a mounted drive. A mounted drive is a drive that is attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter. If you use mounted drives, critical system features may not work as intended. You do not, for example, receive any warnings if the system runs out of disk space.

Before you start: Shut down any existing surveillance software. If you are upgrading, read Upgrade from a previous version (see "Upgrading from one product version to another product version" on page 30) first.

1. Run the installation file.
2. If you have a previous installation of your system or any of the other XProtect Professional VMS products installed, the system detects this installation and informs you that your previous installation will be removed after installing the new version. If you accept this, click **Yes** to continue the installation. All your recordings and configuration from the previous version will be available in the new version.
3. Select language for the installer and then click **Continue**.
4. Select **Trial** to install a trial version of the system software if you do not have a license file yet. If you already have a license file, type the destination of the license file or click **Browse** to locate it on your computer.
5. Read and accept the license agreement, indicate if you want to participate in the Milestone data collection program and indicate if you want to enable access to **Customer Dashboard**.
6. Select **Typical** or **Custom** installation. If you select **Custom** installation, you can select application language, which features to install and where to install them. Let the installation wizard complete.
7. If you have installed a trial version, open the Management Application once the installation is complete and select which of the XProtect Professional VMS Products you want to use, for example XProtect Enterprise.

You can now begin to configure your system. To do so, see Get your system up and running (on page 33).

Install silently

A surveillance system administrator can deploy the system or XProtect Smart Client to users' computers by using tools such as Microsoft Systems Management Server (SMS). With this tool, you can build up databases of hardware and software on local networks. You can then use the databases for distributing and installing software applications over local networks.

To install silently:

1. Locate the XProtect Smart Client .exe file **MilestoneXProtectSmart Client_x64.exe**. Find the file in a subfolder under the folder **httpdocs**. The **httpdocs** folder is located under the folder in which your Milestone surveillance software is installed.

   The path is typically (if you are using an English language version of the XProtect Smart Client):
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\XProtect Smart Client Installer\[version number] [bit-version]\All Languages\en-US

   For example:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\XProtect Smart Client Installer\2014 (64-bit)\All Languages\en-US

2. Run a silent installation using one of the following two options:

a) Run with default parameter settings:

To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and execute following command:

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --quiet

  Your system:

  MilestoneXProtectProfessionalVMS_installer_x64.exe --quiet

This performs a quiet installation of XProtect Smart Client or your system using default values for parameters such as target directory and so on. To change the default settings, see the following:

a) Customize default parameters using an XML argument file as input:

In order to customize the default installation settings, you must provide an XML file with modified values as input. In order to generate the XML file with default values, open a command prompt in the directory where the installation program is located and execute following command:

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --generateargsfile=[full path]args.xml

- Your system:

  MilestoneXProtectProfessionalVMS_installer_x64.exe --generateargsfile=[full path]args.xml

Open the generated args.xml file in a text editor and perform any changes needed. Then execute the following command in the same directory to run a modified version of the silent installation.

- XProtect Smart Client:

  MilestoneXProtectSmart Client_x64.exe --arguments=[full path]args.xml --quiet

- Your system:

MilestoneXProtectProfessionalVMS_installer_x64.exe --arguments= [full path]args.xml --quiet

Install video device drivers

Video device drivers are installed automatically during the initial installation of your system. New versions of video device drivers, known as XProtect Device Pack, are released from time to time and made available for free on the Milestone website. Milestone recommends that you always use the latest version of video device drivers. When you update video device drivers, you can install the latest version on top of any version you may have installed.

When you install new video device drivers, your system cannot communicate with camera devices from the moment you begin the installation until the moment installation is complete and you have restarted the Recording Server service. Usually, the process takes no longer than a few minutes, but Milestone highly recommends that you perform the update at a time when you do not expect important incidents to take place.

To install video device drives:

1. On the system server on which you want to install the new video device drivers version, shut down any running surveillance software, including any running Recording Server service.
2. Run the XProtect Device Pack installation file and follow the wizard.
3. When the wizard is complete, remember to start the Recording Server service again.

If you use the Add Hardware Devices Wizard's Import from CSV File option, you must—if cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. To view a current list of IDs, view the release notes for the XProtect Device Pack used in your organization. Alternatively, visit the Milestone website for the latest information.

Upgrade

About upgrading

If you want to upgrade your system, you can do this in different ways. You can:

- Perform an upgrade from one product version to a newer version of the same product, for example upgrading from XProtect Enterprise 2013 to XProtect Enterprise 2014.
- Perform an upgrade from one XProtect product to another XProtect product, for example upgrading from XProtect Essential to XProtect Professional. You can also downgrade a product if needed.

Upgrading your software gives you access to more or expanded functionality.

About updates

Milestone regularly release service updates that offers improved functionality and support for new devices.

When a new version of your VMS software is available, a message in the yellow notification bar informs you that you can update the software. Milestone recommends that you always install the latest version of your surveillance software to ensure that your software is running as smoothly as possible.

Upgrading from one product version to another product version

About upgrading from one product version to another product version

You can upgrade your entire system configuration from one product version to another, for example from XProtect Enterprise 2013 to XProtect Enterprise 2014 fairly fast and easily. Install the new product on top of the old version without any need to install the previous version.

When you install the new version of your system, it inherits the configuration from the previously installed version/product.Milestone recommends that you make regular backups of your server configuration as a disaster recovery measure. You should also do this when you upgrade your server. While it is rare that you lose your configuration (cameras, schedules, views and more), it **can** happen under unfortunate circumstances. Fortunately, it takes only a minute to back up your existing configuration.

If you use XProtect Professional 6.5, you must upgrade to XProtect Professional 7.0 or newer before you can upgrade to the current version. You must also perform a manual backup of your system configuration before you can upgrade your system.

Note that you do not need to manually remove the old version of your system before you install the new version. The old version is removed when you install the new version. However, you must remove XProtect Basis+ versions earlier than 6.0 manually before installing the new version.

The following describes backing up XProtect Professional 6.5 or earlier. If you need information about how to back up configuration for XProtect Professional 7.0 or newer, see Back up system configuration (on page 194).

1. Create a folder called **Backup** on a network drive, or on removable media.
2. On the system server, open **My Computer**, and navigate to the system's installation folder.
3. Copy the following files and folders into your **Backup** folder:
   - All configuration (.ini) files
   - All scheduling (.sch) files
   - The file **users.txt** (only present in a few installations)
   - Folders with a name ending with **...ViewGroup** and all their content

Note that some of the files/folders may not exist if upgrading from old software versions.

If you installed your system as a custom version to a non-default file-path, make a backup of your existing configuration and restore it to a new installation folder called **[relevant folder]\Milestone Surveillance**. When you run the installer, select **Custom** installation and when you are prompted for an installation folder, select the **[relevant folder]** created for restoring.

Upgrading from one current XProtect Professional VMS product to another current XProtect Professional VMS product

About upgrading from one current XProtect Professional VMS product to another current XProtect Professional VMS product

If you use one of the XProtect Professional VMS Products*, for example XProtect Express and decide that you want to use the additional features and functionality found in a different XProtect VMS product, for example, XProtect Professional, you can upgrade your system in a few steps.

If you are running one XProtect product in trial mode, you can purchase a license for a different product to license that product and to upgrade or downgrade the system if you need to. Your license file decides which XProtect Professional VMS product you can use. This means that if you change VMS product, you do not need to install the new product on top of the existing product as the change of product occurs once you have licensed your software.

When you upgrade from one XProtect product to a more feature-rich XProtect product, you get access to new functionality, but you can also expand on the use of already available functionality. Your settings from the previous product are transferred to the new product. This means that you sometimes need to update the settings of your old product in order to make use of the expanded functionality.

For further information about the various differences between products, check the Milestone website at www.milestonesys.com.

Example: If you upgrade from XProtect Go to XProtect Essential, you should, among other things, be aware of:

- XProtect Smart Client: In XProtect Go, only one instance of the XProtect Smart Client can be connected at a time. When you upgrade, you get the possibility of connecting more instances of the XProtect Smart Client. Since you come from XProtect Go, the Management Application is set to only allow one connected XProtect Smart Client at a time. You can change this setting **manually** in the Management Application. In general, you gain the full use of XProtect Smart Client functionality when you upgrade.
- Number of cameras: XProtect Go allows you to use up to eight cameras at the same time, while you can use many more in XProtect Essential and other XProtect VMS products. The number of cameras you have added are inherited by the upgraded product, but you must, of course, add any additional cameras to the Management Application yourself.

* XProtect Professional VMS Products cover the following products: XProtect Enterprise, XProtect Professional, XProtect Express, XProtect Essential and XProtect Go.

About removing system components

To remove the entire surveillance system (that is the surveillance server software and related installation files, the video device drivers, XProtect Download Manager, XProtect Smart Client, the Event Server service and the Milestone Mobile server) from your server, follow the normal Windows procedure for uninstalling programs (see the Windows Help for more information).

You can also remove individual components, such as XProtect Smart Client and video drivers by using the standard Windows procedure for uninstalling programs.

If you remove your surveillance system, your recordings are not removed. They remain on the server even after the server software has been removed. Configuration files also remain on the server. This allows you to reuse your configuration if you install the system again at a later time.

First time use

Get your system up and running

This checklist outlines the tasks typically involved when you set up a working system.

Note that although the information is presented as a checklist, a completed checklist does not in itself guarantee that the system matches your exact needs. To make the system match the needs of your organization, Milestone highly recommends that you monitor and adjust the system once it is running.

For example, it is often a good idea to spend time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (such as day or night, windy or calm wather). Do this once the system is running. The setup of events and associated actions typically also depends on your organization's needs.

You can print and use this checklist as you go along.

☐	**Install your system** See Install surveillance server software **(see "**Install your system software**" on page 27).** If you are upgrading an existing version of your system, see Upgrade from a previous version **(see "**Upgrading from one product version to another product version**" on page 30).**
☐	**Register your software** You may not need to go through this step as your vendor often takes care of the process for you. You must first register your software and next activate your licenses.
☐	**Open the Management Application** Open the Management Application after installation to begin setting up your system features.
☐	**Verify initial configuration of cameras and other hardware devices** When you open your system for the first time, the Getting Started wizard assists you with a quick way to add hardware devices (cameras, video encoders and more) to your system and configure them with proper user names and passwords. See Getting started wizard (see "Automatic configuration wizard" on page 39).
☐	**Configure cameras** You can specify a wide variety of settings for each camera connected to your system. Settings include video format, resolution, motion detection sensitivity, where to store and archive recordings, any pan-tilt-zoom (PTZ) preset positions, association with microphones, speakers and more. See About video and recording configuration (on page 64).
☐	**Configure events, input and output** If required, use system events, for example based on input from sensors, to automatically trigger actions in your system. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, making PTZ cameras move to specific preset positions. Also use events to activate hardware output, such as lights or sirens. See Overview of events.

☐	**Configure scheduling** Set up when do you want to archive and if you want cameras to transfer video to your system at all times, and other cameras to transfer video only within specific periods of time as well as when specific events occur. Also specify when you want to receive notifications from the system. See Configure general scheduling and archiving (on page 131) and Configure camera-specific schedules (on page 67).
☐	**Configure clients' access to your system** A number of different client applications are included with your system. Specify whether you want clients to access the system server from the Internet, how many clients you want to be able to connect simultaneously and more. See Configure server access (on page 159).
☐	**Configure master/slave servers** You only need to follow this step if you want to run several servers together and the functionality is only available if you run XProtect Enterprise or XProtect Professional. A master/slave setup allows you to combine several servers and extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server. In such a setup, clients still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers. See Configure master and slave servers (on page 161).
☐	**Configure users** Specify who should access your system and how. Set a password protection for the Management Application if needed. Decide who should have client access which rights they should have. See Configure User Access wizard (see "Manage user access wizard" on page 55), Add basic users (on page 163), Add user groups (on page 164) and Configure user and group rights (on page 165).
☐	**Configure XProtect Download Manager** Manage which features users see on a targeted welcome page when they connect to the system server. The features can include access to client applications, additional client language versions, plug-ins and more. XProtect Download Manager comes with a default configuration that ensures that users get access to XProtect Smart Client in the same language as your system server. See Use XProtectDownload Manager

The above list represents the configuration steps that most administrators are likely to cover. You can, of course, do more configuration, for example if your organization wants to use the Matrix (see "About Matrix video sharing" on page 136) video-sharing feature.

Best practices

About protecting recording databases from corruption

You can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While it is good to have such options, Milestone recommends that you take steps to ensure that your camera databases do not become corrupted.

Power outages: use a UPS

The single-most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When you assess your needs, however, bear in mind the amount of runtime you require the UPS to be able to provide if the power fails. Saving open files and shutting down an operating system properly may take several minutes.

Windows Task Manager: be careful when you end processes

When you work in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking **End Process** in the Windows Task Manager, the process is not be given the chance to save its state or data before it is terminated. This may lead to corrupt camera databases.

Windows Task Manager typically displays a warning if you attempt to end a process. Unless you are absolutely sure that ending the process is not going to affect the surveillance system, click **No** when the warning message asks you if you really want to terminate the process.

Hard disk failure: protect your drives

Hard disk drives are mechanical devices and are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)
- Strong magnetic fields (avoid)
- Power outages (make sure you use a UPS (on page 207))
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water and more (avoid).

About saving changes to the configuration

As you set up your system, you must save any changes you make to the configuration in order for these to be applied to the system. When you change the configuration in the Management Application, for example in the **Camera Summary** or **User Properties**, a yellow notification bar informs you that you have made changes to the configuration. The bar appears in order to make sure that your

changes are applied to the system. If you want to apply the changes, click **Save**. If you do not want to save your changes, click **Discard**.

Once you have made changes to the configuration of your Management Application and saved these, your system contacts the system services (such as the Recording Server service and the Image Server service). If you make changes to your configuration, for example if you change the name of a camera or change motion detection settings, the relevant system services load the new configuration and the changes appear in your client immediately. In contrast, more resource-demanding configuration changes, for example if you add a new event, require that you restart the relevant services before they work properly.

If you need to restart services, your system carries out the restart automatically once you have saved the changes. If you make changes to settings in the Milestone Mobile server, your system applies all changes when you click **Save,** without restarting the Milestone Mobile server service.

IMPORTANT: While your system restarts services, you cannot view or record video. Restarting services typically only takes a few seconds, but in order to minimize disruption, you may want to restart services at a time when you do not expect that any important incidents take place. Users connected to your system through clients can remain logged in during the restart of services, but may experience a short video outage.

Note that the system stores changes in a restore point (see "Restore system configuration from a restore point" on page 200) (so that you can return to a working configuration if something goes wrong).

About using the built-in help

To use your system's built-in help, click the **Help** button in the Management Application's toolbar or press the **F1** key on your keyboard.

The help system opens in your default Internet browser and allows you to switch between the help and your system itself. The help system is context-sensitive. This means that when you press F1 for help while you work in a particular dialog, the help system displays help that matches that dialog.

Navigate the built-in help system

To navigate between the contents of the help system, use the help tabs: **Contents**, **Index, Search,** or use the links inside the help topics.

- **Contents:** navigate the help system based on a tree structure.
- **Index:** contains an alphabetical indexation of help topics.
- **Search:** search for help topics that contain particular terms of interest. For example, you can search for the term **zoom** and every help topic that contains the term **zoom** is listed in the search results. When you double-click a help topic title in the search results list, the relevant topic opens.

Print help topics

If you need to print a topic, use your Internet browser's printing function. When you print a help topic, it is printed as you see it on your screen. This means that if a topic contains links that expand when you click on them (drop-down links) and you want the information in the drop-down links shown in your print output, you must click each relevant drop-down link to display the text to include it when you print. This allows you to create targeted printouts that contain exactly the amount of information you need.

About restarting services

Some changes in the Management Application require that your system restarts the Image Server service or Recording Server service. See a list of these below:

Image Server	Recording Server
Change of port number	Changing licenses
Maximum number of clients	Changing event database path
Enabling or disabling of master servers	Turning on manual recording
Adding or removing slave servers	Starting on remote
Change of log path	Enabling and disabling of notifications
Change of license	Changing events
Change of privacy mask	Changing outputs
Removal of hardware devices	Adding or removing a dynamic archiving path
Turning evidence collection mode on or off. XProtect Enterprise only.	Adding or removing archiving time
	Changing of scheduling
	Setting up the Matrix functionality
	Replacing hardware devices
	Changing camera driver
	Changing camera IP address
	Deletion of all devices
	Enabling or disabling of alarm on Customer Dashboard
	Turning evidence collection mode on or off. XProtect Enterprise only.

Monitor storage space usage

To view how much storage space you have on your system—and not least how much of it is free—do the following:

1. Expand **Advanced Configuration**, and select **Cameras and Storage Information**.

2. View the **Storage Usage Summary** for information about, which drives are available, what drives are used for, the size of each drive, as well as how much video data, other data, and free space there is in each drive.

View video from cameras in Management Application

You can view live video from single cameras directly in the Management Application:

1. Expand **Advanced Configuration**, and expand **Cameras and Storage Information**.
2. Select the relevant camera to view live video from that camera. Above the live video, you find a summary of the most important properties for the selected camera. Below the live video, you find information about the camera's resolution and average image file size. For cameras using MPEG or H.264, you also see the bit rate in Mbit/second.

IMPORTANT: Viewing of live video in the Management Application may under certain circumstances affect any simultaneous recording from the relevant camera. Especially three scenarios are important to consider:

- Some cameras supporting multistreaming may halve their frame rate or respond with other negative effects if you open a second stream.

- If a camera delivers live video in a very high quality, de-coding of images may increase the load on the Recording Server service, which may in turn affect ongoing recordings negatively.

- Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

Getting started

About the Getting started page

The Getting started window is always shown when you open the Management Application. The Getting started page provides you with an easy way to go through wizards and serves as a place of reference for users.

To know how many of your system's camera licenses you are using, or to know the expiration date of your Software Upgrade Plan (SUP), you can find this information in the bottom-left and bottom-center columns on the Getting started page. To access information about your SUP, you must be connected to the Internet.

You can also access and view video tutorials that show and explain how to go through each step of your system's wizards. To access these, click the **View tutorials** link to this in the bottom-right column. The link takes you to an external web page with video tutorials for your system.

Automatic configuration wizard

The **Automatic configuration** wizard is for easy configuration for first time use of the system. Use the wizard to automatically add cameras to your system using this step-by-step procedure.

Automatic configuration wizard: First page

When you open the Management Application for the first time, the Automatic configuration wizard opens to guide you through the process of adding hardware devices to your system. If you are new to the system, click **Yes, configure** to scan your network for available cameras and configure your system. To exit and use a more advanced way of adding devices to your system, click **Skip** to leave the wizard and go to the Management Application to get more options for setting up your system's device configuration.

Automatic configuration wizard: Scanning options

Choose where you want your system to scan for cameras and devices.

By default, the **Scan local network** checkbox is selected, which means that you only scan your local network for devices. However, if you know the IP address or a range of IP addresses to which cameras and devices are attached, specify these by clicking the Plus icon next to **Add the IP addresses or IP ranges to be scanned**. You can add more than one range of IP addresses if you need to.

Automatic configuration wizard: Select hardware manufacturers to scan for

If you know the specific manufacturer of your hardware device(s), select these in the dropdown on this page. You can select as many manufacturers as you want to.

Note: By default, all manufacturers are selected. If you want to reduce the scanning time or know the specific manufacturers of your cameras, only select the checkboxes that represents these manufacturers.

Automatic configuration wizard: Scanning for hardware devices

Scanning for hardware devices that match your selected manufacturers begins. A status bar indicates how far in the scan process you are. Once scanning for cameras and devices is complete, you may need to provide user name and password for your selected devices or cameras. When you have typed in the relevant credentials, click the **Verify** button to add the device to your system.

Note: Not all devices and cameras need a user name and password. You can add such devices to your system without any need to type in credentials.

Automatic configuration wizard: Continue after scan

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

When the system has finished configuring storage, you are given the option to automatically add new cameras to your system as they are detected on the network. Enabling this allows you to set up your system so that any devices or cameras are automatically set up for you in the future as soon as they are connected to your network. Note that not all devices and cameras support automatic discovery. If your device/camera does not show up automatically after you have connected it to your network, you must add it manually.

To go directly to XProtect Smart Client once you have completed the wizard, select the check box in the bottom-left corner of the wizard page.

Add hardware wizard

You add cameras and other hardware devices, such as video encoders, to your system through the **Add Hardware wizards**. If the hardware device has microphones or speakers attached, the tool automatically adds these as well.

You may have a limit on the number of cameras you can use in your system. Note that you can add more cameras than you are allowed to use. If you use video encoder devices on your system, note that many video encoder devices have more than one camera connected to them. For example, a fully used four-port video encoder counts as four cameras.

The wizard offers you two different ways of adding cameras:

Name	Description
Scan for hardware	Scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add hardware: Scan for hardware (see "Express" on page 41)

Name	Description
Manually specify the hardware to add	Specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords and more. See Add hardware: Manually specify the hardware to add (see "Manual" on page 42). Alternatively, import data about cameras as comma-separated values from a file. An effective method if you set up several systems. See Add hardware: Import from CSV File (see "Import from CSV file" on page 43).

Express

Note: Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, your system can quickly recognize relevant hardware devices, such as cameras and video encoders, and include them in a scan.

The **Scan for hardware** method gives you the option to scan your network for relevant hardware devices and quickly add them to your system in just a few steps.

Choose between these two options for adding hardware:

- **Scan local network**: Perform an automated scan for available hardware on your local network that support device discovery, on the part of your network (subnet) where the system server itself is located.
- **Add IP address or IP range to be scanned:** Add hardware to your system by indicating IP ranges and ports from which the system begin scanning for hardware.

To use the **Scan local network** method, your system server and your cameras must be on the same layer 2 network. This means that it must be on a network where all servers, cameras, and so on can communicate without the need for a router. The reason for this is that device discovery relies on direct communication between the system server and the cameras. If you use routers on your network, specify the IP range where you hardware is located using the **Add IP address or IP range to be scanned**-option or choose one of the Manually specify the hardware to add (see "Manual" on page 42)-methods.

Add hardware: Scanning options

Choose where you want your system to scan for cameras and devices.

By default, the **Scan local network** checkbox is selected, which means that you only scan your local network for devices. However, if you know the IP address or a range of IP addresses to which cameras and devices are attached, specify these by clicking the Plus icon next to **Add the IP addresses or IP ranges to be scanned**. You can add more than one range of IP addresses if you need to.

Add hardware: Select hardware manufacturers to scan for

If you know the specific manufacturer of your hardware device(s), select these in the dropdown on this page. You can select as many manufacturers as you want to.

Note: By default, all manufacturers are selected. If you want to reduce the scanning time or know the specific manufacturers of your cameras, only select the checkboxes that represents these manufacturers.

Hardware detection and verification

Scanning for hardware devices that match your selected manufacturers begins. A status bar indicates how far in the scan process you are. Once scanning for cameras and devices is complete, you may need to provide user name and password for your selected devices or cameras. When you have typed in the relevant credentials, click the **Verify** button to add the device to your system.

Note: Not all devices and cameras need a user name and password. You can add such devices to your system without any need to type in credentials.

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

Manual

With the **Manually specify the hardware to add** method, you can specify details about each hardware device separately. This options is a good choice if you only want to add a few hardware devices, and you know their IP addresses, user names and passwords and so on. Similarly, automated searches on the local network using the **Scan for hardware** option might not work for all cameras, for example cameras using the system's **Universal Driver**. For such cameras, you must add these to the system manually.

Alternatively, choose **Import CSV file** (see "**Import from CSV file**" on page 43). This option lets you import data about hardware devices and cameras as comma-separated values (CSV) from a file. This is a highly effective method if you set up several similar systems.

Information, driver selection and verification

Specify information about each hardware device you want to add:

Name	Description
IP Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.

Name	Description
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
Password	Password required to access the administrator account. Some hardware devices do not require user name/password for access.
Driver	The driver to scan for for your hardware device. By default, the wizard shows the Autodetect option. The Autodetect option finds the relevant driver automatically. Select a manufacturer if you know the specific manufacturer to reduce scanning time.

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

Import from CSV file

Import data about hardware devices and cameras as comma-separated values (CSV) from a file. This is a highly effective method if you set up several similar systems.

Add Hardware Devices wizard - Import from CSV File - example of CSV file

The following is an example of a CSV file for use when cameras and server are online. It includes the parameters **HardwareAddress, HardwarePort, HardwareUsername, HardwarePassword** and **HardwareDriverID.** Note that HardwareUserName and HardwareDriverID are optional parameters. You can leave out the HardwareUsername if you have not changed the default HardwareUsername for the device. HardwareDriverID is an optional field. If empty, it is automatically set to autodetect.

```
HardwareAddress;HardwarePort;HardwareUsername;HardwarePassword;Hardwa
reDriverID;
192.168.200.220;80;root;pass;128;
192.168.200.221;80;user;password;165;
192.168.200.222;80;r00t;pass;172;
192.168.200.223;80;;p4ss;
192.168.200.224;80;usEr;pASs;
```

Add hardware: Import from CSV file - CSV file format and requirements

The CSV file must have a header line (determining what each value on the following lines is about), and the following lines must each contain information about one hardware device only. A minimum of information is always required for each hardware device:

Name	Description
HardwareAddress	IP address of the hardware device.
HardwareUsername	User name for hardware device's administrator account.
HardwarePassword	Password for hardware device's administrator account.
HardwareDriverID	If cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. Example: **ACTi ACD-2100 105** indicates that you should use **105** as the ID if adding an ACTi ACD-2100 hardware device.

Existing configuration parameters that are not specified in CSV file remain unchanged. If a parameter value for an individual camera in the CSV file is empty, the existing parameter value remains unchanged on that camera. Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file.

The following applies for the information present in CSV files:

- The first line of the CSV file must contain the headers, and following lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names and similar items must be unique, and must not contain any of the following special characters: **< > & ' " \ / : * ? | [ ]**
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored

Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed. Even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings.

Configure storage wizard

The **Video storage** step helps you quickly configure your cameras' video and recording properties.

Configure storage: Video settings and preview

Control bandwidth, brightness, compression, contrast, resolution, rotation and more in Video settings. Use the list on the left side of the wizard window to select a camera and adjust its video settings. Then select the next camera and adjust its settings. Video settings are to a large extent camera-specific, so you must configure these settings individually for each camera.

Click **Open Settings Dialog** to configure the camera's settings in a separate dialog. When you change video settings, they are applied immediately. This means that—for most cameras—you can immediately see the effect of your settings in a preview image. However, it also means that you cannot undo your changes by exiting the wizard. For cameras set to use the video formats MPEG or H.264, you can typically select which live frame rate to use for the camera.

Video settings may feature an **Include Date and Time** setting. If set to **Yes**, date and time from the camera are included in the video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and XProtect system time may therefore not correspond fully, and this may occasionally lead to confusion. As your system time-stamps all frames upon reception, and exact date and time information for each image is already known, Milestone recommends that you set it to **No**.

Note: For consistent time synchronization, you may automatically synchronize camera and system time through a time server if your camera supports this.

Configure storage: Online schedule

Specify when each camera should be online. An online camera is a camera that transfers video to the server for live viewing and further processing. The fact that a camera is online does not in itself mean that your system records video from the camera (configure recording settings on one of the following pages). By default, cameras you add to your system are automatically online (**Always on**), and you only need to modify their online schedules if you require cameras to be online only at specific times or events. Note, however, that you can change this default as part of the scheduling options (on page 133).

For each camera, you can initially select between two online schedules:

- **Always on:** The camera is always online.
- **Always off:** The camera is never online.

If these two options are too simple for your needs, use the **Create / Edit...** button to specify online schedules according to your needs, and then select these schedules for your cameras. This way, you can specify whether cameras should be online within specific periods of time, or whether they should start and stop transferring video when specific events occur within specific periods of time.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Apply the value from the template to selected cameras.

Configure storage: Live and recording settings (motion JPEG cameras)

This wizard page only appears if one or more of your cameras use the MJPEG video format.

Select pre- and post-recording, which allows you to store recordings from the time before and after detected motion and/or specified events. Also specify which frame rates to use for each camera (XProtect Enterprise and XProtect Professional only).

Properties available in all XProtect software versions:

Name	Description
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 126) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

Properties available in XProtect Enterprise and XProtect Professional only:

Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.

Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Properties available in all XProtect software versions:

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Apply the value from the template to selected cameras.

Configure storage: Live and recording settings (MPEG cameras)

This wizard page only appears if one or more of your cameras use the MPEG video format.

Specify which frame rate to use for each camera, and whether to record all frames or keyframes only. You can also select pre- and post-recording, allowing you to store recordings from periods preceding and following detected motion and/or specified events.

Note that all of the properties can also be specified individually for each camera.

Properties available in all XProtect software versions:

Name	Description
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.

Name	Description
Record on	Select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 86) and scheduled to be online (see "Online period" on page 134) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 96) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. Use the **Configure events** list, located below the other fields to define events that suit your needs. • **Motion Detection and Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 126) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.

Name	Description
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

Properties available in XProtect Enterprise and XProtect Professional only:

Keyframe Only	Select **Keyframe only** if you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Apply the value from the template to selected cameras.

Configure storage: Drive selection

Specify which drives you want to store cameras' recordings on. You can specify separate drives/paths for recording and archiving (see "About archiving" on page 126).

Properties available for all XProtect software versions:

Name	Description
Drive	Letter representing the drive in question, for example C:.

Name	Description
Purpose	Select what you want to use the drive for: **Not in use:** Do not use the drive. **Recording:** Only available if the drive is a local drive on the XProtect Professional server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Professional. **Archiving:** Use the drive for archiving. For archiving, it is generally a good idea to use a drive which has plenty of space. With dynamic path selection for archives (see description in the following), you do not have to worry about drive space. **Rec. & Archiving:** Only available if the drive is a local drive on the XProtect Professional server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Professional as well as for archiving.
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 126). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Total Size	Total size of the drive.
Free Space	Amount of unused space left on the drive.

Name	Description
Dynamic path selection for archives	If using this option (highly recommended), you should select a number of different local drives for archiving. If the path containing the XProtect Professional database is on one of the drives you have selected for archiving, XProtect Professional will always try to archive to that drive first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.
Archiving Times	Specify when you want XProtect Professional to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.
Properties available in XProtect Enterprise and XProtect Professional only:	
Network Drive	Lets you add a network drive to the list of drives. First specify the network drive, then click **Add** (the button becomes available when you specify a network drive) . Note that network drives cannot be used for recording, only for archiving.

Configure storage: Recording and archiving settings

Select recording and archiving (see "About archiving" on page 126) paths for each individual camera.

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

Name	Description
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.

Name	Description
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 126). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention time	Total amount of time for which you want to keep recordings from the camera (that is, recordings in the camera's database as well as any archived recordings). Default is 7 days. Retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Apply the value from the template to selected cameras.

Adjust motion detection wizard

The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

Adjust motion detection: Exclude regions

Disable motion detection in specific areas of cameras' views in the Exclude regions section of the wizard. Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if a camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

For each camera for which exclude regions are relevant, use the list in the left side of the wizard window to select the camera and define its exclude regions. Exclude regions are camera-specific, and you must configured motion detection individually for each camera on which they are required.

When you have selected a camera, you see a preview from the camera. You define regions to exclude in the preview, which is divided into small sections by a grid.

- To make the grid visible, select the **Show Grid** check box.
- To define exclude regions, drag the mouse pointer over the required areas in the preview while pressing the mouse button down. Left mouse button selects a grid section and right mouse button clears a grid section. Selected areas are highlighted in blue.

If you use the **Include All** button, you can quickly select all grid sections in the preview. This can be advantageous if you want to disable motion detection in most areas of the preview, in which case you can clear the few sections in which you do not want to disable motion detection. With the Exclude All button you can quickly clear all sections.

Adjust motion detection: Motion detection

Motion detection is a key element in most surveillance systems. Depending on your configuration, motion detection settings may determine when video is recorded (saved on the surveillance system server), when notifications are sent, when output (a light or siren) is triggered and more.

It is important that you find the best possible motion detection settings for each camera to avoid unnecessary recordings, notifications and more. Depending on the physical location of your cameras, it is a good idea to test settings under different physical conditions (day/night, windy/calm weather and similar conditions).

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

You can configure motion detection settings for each camera, or for several cameras at once. Use the list in the left pane of the wizard window to select cameras. To select several cameras at a time, press **CTRL** or **SHIFT** while you select. When you select a camera, you see a preview from that camera. If you select several cameras, you see a preview from the last camera you select. A green area in the preview indicates motion.

Properties available in all XProtect software versions:

Name	Description
Sensitivity	Adjust the **Sensitivity** slider so that irrelevant background noise is filtered out, and only real motion is shown in green. Alternatively, specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting. The slider determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. The more you drag the slider to the left, the more of the preview becomes green. This is because with high sensitivity, even the slightest pixel change is regarded as motion.
Motion	Adjust the **Motion** slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the **Level** bar above the sliders. The black vertical line serves as a threshold. When motion is above (to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection. Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting. The more you drag the slider to the left, the more positive motion detections you see because less change will be needed to trigger a positive motion detection. The number of positive motion detections may also affect the amount of video you record, the amount of notifications you receive and more.
Detection interval	Specify how often motion detection analysis is carried out on video from the camera. The default is every 240 milliseconds (close to once a quarter of a second). The interval is applied regardless of your cameras' frame rate settings. Adjusting this setting can help lower the amount of system resources used on motion detection.

Name	Description
Detection resolution	Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.
Properties available in XProtect Enterprise only:	
Keyframe Only	Select **Keyframe only** if you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection.

Manage user access wizard

Use the **Manage user access step** to add individual users so they can access the system and its clients. The access summary at the end of the wizard lists the cameras your users have access to.

Important: When you use the wizard, all users you add get access to all cameras, including any new cameras added at a later stage. You can, however, specify access settings, users and user rights (see "Configure user and group rights" on page 165) separately, see Configure server access (on page 159). You cannot add users to groups (see "Add user groups" on page 164).

Manage user access: Basic and Windows users

Active Directory® is supported in XProtect Enterprise 2013+ and XProtect Professional 2013+ only.

You can add client users in two ways. You can combine these if you need to.

Name	Description
Basic user	Create a dedicated surveillance system user account with basic user name and password authentication for each individual user.
Windows user	Import users defined locally on the server or from Active Directory, and authenticate them based on their Windows login.

Note: You must define users as local PC users on the server and disable simple file sharing on the server.

Add Basic users

1. Specify a user name and password, and click the **Add Basic User** button. Repeat as required.

Add Windows users

1. Click **Add Windows User...** to open the **Select Users or Groups** dialog. You can only make selections from the local computer, even if you click the **Locations...** button.

2. In **Enter the object names to select,** enter the user name(s), then use the **Check Names** feature to verify the user name. If you enter several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**

3. When done, click **OK**.

Important: When a user who has been added from a local database logs in with a client, the user should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001, not: PC001/USER001. The user should, of course, still specify a password and any relevant server information.

Manage user access: Access summary

The access summary lists which cameras your users have access to. When you use the wizard, all users you have added have access all to cameras, including any new cameras added at a later stage. You can, however, limit individual users' access to cameras by changing their individual rights (see "Configure user and group rights" on page 165).

Advanced configuration

Hardware devices

About hardware devices

You add cameras and other hardware devices, such as video encoders, to your system through the **Add Hardware Devices...** wizard (see "Add hardware wizard" on page 40). If microphones or speakers are attached to a hardware device, they are automatically added as well (if your XProtect version supports this).

About microphones

In your system, **Microphones** are typically attached to hardware devices, and therefore physically located next to cameras. Operators, with the necessary rights, can then listen to recordings through the XProtect Smart Client (provided the computer running the XProtect Smart Client has speakers attached). You manage microphones on your system, meaning you can always manage the microphones attached to cameras, **not** microphones attached to XProtect Smart Client operators' computers.

If you have added more microphones to your system than you need, you can hide the ones you do not need by right-clicking the relevant microphone or speaker and select **Hide**. If you need the hidden microphone again, you can right-click the overall microphone icon and select **Show Hidden Items**.

About speakers

Speakers are attached to devices, and typically physically located next to cameras. They can typically transmit information to people near a camera. Operators with the necessary rights can talk through speakers using XProtect Smart Client (provided the computer running XProtect Smart Client has a microphone attached).

Example: An elevator is stuck. Through a camera mounted in the elevator, XProtect Smart Client operators can see that there is an elderly lady in the elevator. A microphone attached to the camera records that the lady says: “I am afraid. Please help me out!” Through a speaker attached to the camera, operators can tell the lady that: “Help is on its way. You should be out in less than fifteen minutes.”

If you have added more speakers to your system than you need, you can hide the ones you do not need by right-clicking the relevant peaker and select **Hide**. If you need the hidden speaker again, you can right-click the overall speaker icon and select **Show Hidden Items**.

About recording audio

If you record audio, it is important that you note the following:

- Your system only records incoming audio (from microphones). The system does not record outgoing audio (from speakers).

- Audio recording affects video storage capacity. The system records audio to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since your system automatically archives data if the database becomes full. However, you may need additional archiving space if you record audio.
    - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) are stored in one record in the database. Each second of audio is stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
    - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

The above examples are simplified. The exact available video storage capacity also depends on GOP/JPEG and audio kilobyte size.

About dedicated input/output devices

You can add a number of dedicated input/output (I/O) hardware devices to your system. For information about which I/O hardware devices your system supports, see the release notes.

When you add I/O hardware devices, input on them can be used for generating events in your system and events in your system can be used for activating output on the I/O hardware devices. This means that you can use I/O hardware devices in your events-based system setup in the same way as a camera.

With certain I/O hardware devices, the surveillance system must regularly check the state of the hardware devices' input ports to detect whether input has been received. Such state checking at regular intervals is called **polling**. The interval between state checks, called a **polling frequency**, is specified as part of the general ports and polling properties (see "Ports and polling" on page 116). For such I/O hardware devices, the polling frequency should be set to the lowest possible value (one tenth of a second between state checks). For information about which I/O hardware devices require polling, see the release notes.

Show or hide microphones or speakers

If you have added more microphones or speakers to your system than you need, you can hide the ones you do not need by right-clicking the relevant microphone or speaker and select **Hide**. If you need the hidden microphone/speaker again, you can right-click the overall microphone or speaker icon and select **Show Hidden Items**.

Configure hardware devices

Once you have added hardware devices, you can specify/edit device-specific properties, such as the IP address, which video channels to use, which COM ports to use for controlling attached PTZ (pan-tilt-zoom) cameras, whether to use 360° lens technology, etc.

1. Expand **Advanced Configuration**, expand **Hardware Devices**, right-click the relevant hardware device, and select **Properties**.
2. Specify Name and video channels, Network, device type and license (see "Network, device type, and license" on page 62), PTZ device (see "PTZ device (properties)" on page 63), and 360° lens (see "Fisheye" on page 100) properties as required.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Delete hardware devices

IMPORTANT: If you delete a hardware device, you not only delete all cameras, speakers and microphones attached to the hardware device. You also delete any recordings from cameras on the hardware device.

1. Expand **Advanced Configuration**, expand **Hardware Devices**, right-click the hardware device you want to delete, and select **Delete Hardware device**.
2. Confirm that you want to delete the hardware device and all its recordings.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.
4. Restart (see "Start and stop services" on page 170) the Recording Server service.

Alternately, you can also consider disabling the individual cameras, speakers or microphones connected to the hardware device:

1. Expand **Advanced Configuration**, expand **Hardware Devices**, and expand the relevant hardware device.
2. Right-click the camera, microphone or speaker that you want to disable, and select **Disable**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.
4. Restart (see "Start and stop services" on page 170) the Recording Server service.

About replacing hardware devices

If you need to, you can replace a hardware device that you have added and configured on your system with a new one, for example to replace a physical camera on your network.

Open the Replace Hardware Device wizard (see "About the Replace Hardware Device wizard" on page 60), which helps you through the entire replacement process on the surveillance system server, including:

- Detecting the new hardware device

- Specifying license for the new hardware device
- Deciding what to do with existing recordings from the old hardware device

About the Replace Hardware Device wizard

Use the Replace Hardware Device wizard to replace a hardware device that you have previously added to and configured on your surveillance system. To open the Replace Hardware Device wizard, right-click the device that you want to replace and select **Replace Hardware Device**. The wizard is divided into the New hardware device information page and the database action page.

New hardware device information

Specify details about the new hardware device:

Name	Description
IP Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
Password	Password required to access the administrator account. Some hardware devices do not require user name/password for access.

To specify which device driver to use for the new hardware device, you can:

- Select the video device driver in the **Hardware device type** list, and then click **Auto-detect/Verify Hardware Device Type** to verify that the driver matches the hardware device.

  - or -

- Click **Auto-detect/Verify Hardware Device Type** to automatically detect and verify the right driver.

When the right driver is found, the **Serial number (MAC address)** field displays the MAC address of the new hardware device. When done, click **Next**.

Camera and database action

On the last page of the Replace Hardware wizard, decide what to do with the camera and the database containing recordings from the camera attached to the old hardware device. For multi-camera devices, such as video encoders, you must decide what to do for each video channel on the new hardware device.

The table in the left side of the wizard page lists available video channels on the new hardware device. For a regular single-camera hardware device, there are only one video channel. For video encoders, there are typically several video channels.

1. For each video channel, use the table's **Inherit** column to select which camera from the old hardware device should be inherited by the new hardware device.

2. Decide what to do with camera databases. You have three options:

   - **Inherit existing database(s):** The cameras you selected to be inherited by the new hardware device inherit camera names, recordings databases as well as any archives from the old hardware device. Databases and archives are renamed to reflect the new hardware device's MAC address and video channels. The rights of users with access to the inherited cameras are automatically updated so they can view both old and new recordings. Users do not notice the hardware device replacement since camera names remain the same.

   - **Delete the existing database(s):** The databases of the cameras you selected to be inherited by the new hardware device are not deleted. New databases are created for future recordings, but it is not possible to view recordings from before the hardware replacement.

   - **Leave the existing database(s):** The databases of the cameras you selected to be inherited by the new hardware device are not deleted. New databases are created for future recordings, but even though the old databases still exist on the System server, it is not possible to view recordings from before the hardware replacement. Should you later want to delete the old databases, you must delete this manually.

3. If the new hardware device has fewer video channels than the old hardware device, it is not possible for the new hardware device to inherit all cameras from the old hardware device. When that is the case, you are asked what to do with the databases of cameras that could not be inherited by the new hardware device. You have two options:

   - **Delete the databases for the cameras that are not inherited:** The databases of the cameras that could not be inherited by the new hardware devices are deleted. It is not possible to view recordings from before the hardware replacement. New databases are, of course, created for future recordings by the new hardware devices.

   - **Leave the databases for the cameras that are not inherited:** The databases of the cameras that could not be inherited by the new hardware devices are not deleted. Even though the old databases still exist on the System server, it is not possible to view recordings from before the hardware replacement. Should you later want to delete the old databases, you must delete this manually. New databases will, of course, be created for future recordings by the new hardware devices.

4. Click **Finish**. When you are ready, restart the Recording Server service. The hardware replacement are not evident in clients until you restart the Recording Server service.

Speaker properties

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you can determine when to record audio. Your choice applies for all cameras on your system.

Name	Description
Enabled	Speakers are by default enabled, meaning they can transfer audio to your system. If required, you can disable an individual speaker, in which case no audio is transferred from the speaker to the system.
Speaker name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Hardware properties

Hardware name and video channels

When you configure hardware devices, specify the following properties:

Name	Description
Hardware name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Video channel # enabled	Enable/disable each of the selected hardware device's video channels. Many hardware devices only have a single video channel, in which case only one channel will be listed. Other hardware devices—typically video encoder devices—have several video channels.

If some of the channels are unavailable, this is because you are not licensed to use all of a video encoder device's channels.

Example: You have a video encoder device with four channels, but your license for the device only allows you to use two of them. In that case, you can only have two channels enabled at a time, while the two other channels are disabled. Note that you are free to select which two channels you want to enable. Contact your Milestone vendor if you need to change your number of licenses.

Network, device type, and license

When you configure hardware devices (on page 59), specify the following properties:

Name	Description
IP Address	IP address or host name of the hardware device.

Name	Description
HTTP Port	Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select **Use default HTTP port**.
FTP port	Port to use for FTP communication with the hardware device. Default port is port 21. To use the default port, select **Use default FTP port**.
User name	Only relevant when you have selected **Server requires login**. Specify the user name required for using the SMTP server.
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
Password	Password for the hardware device's administrator account, a.k.a. the root password.
Hardware type	Read-only field displaying the type of video device driver used for communication with the hardware device.
Serial number (MAC address)	Read-only field displaying the serial number of device. The serial number is usually identical to the 12-character hexadecimal MAC address of the hardware device (example: 0123456789AF).
License information	The current license status for the hardware.
Replace Hardware Device	Opens a wizard (see "About the Replace Hardware Device wizard" on page 60), with which you can replace the selected hardware device with another one if you need to. This can be relevant if you replace a physical camera on your network. The wizard helps you take all relevant issues into account: for example, deciding what to do with recordings from cameras attached to the old hardware device, etc.

PTZ device (properties)

The PTZ Device tab is only available if you configure (see "Configure hardware devices" on page 59) video encoder hardware devices on which the use of PTZ (pan-tilt-zoom) cameras is possible:

Name	Description
Connected cameras have Pan-tilt-zoom capabilities	Select the checkbox if any of the cameras attached to the video encoder device is a PTZ camera.

Name	Description
PTZ type on COM#	If a PTZ camera is controlled through a COM port, select the relevant option. Options are device-specific, depending on which PTZ protocols the device uses. Select None if you have no PTZ cameras controlled through COM ports.

The table in the lower half of the dialog contains a row for each video channel on the hardware device. First row from the top corresponds to video channel 1, second row from the top corresponds to video channel 2, etc.

Name	Description
Name	Name of the camera attached to the video channel in question.
Type	Select whether the camera on the selected camera channel is fixed or moveable: • **Fixed**: Camera is a regular camera mounted in a fixed position • **Moveable**: Camera is a PTZ camera
Port	Available only if **Moveable** is selected in the **Type** column. Select which COM port on the video encoder to use for controlling the PTZ camera.
Port Address	Available only if **Moveable** is selected in the **Type** column. Lets you specify port address of the camera. The port address will normally be 1. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the documentation for the camera.

Cameras and storage information

About video and recording configuration

Once you have added hardware devices and attached cameras, you can configure video and recording settings in three ways:

Name	Description
Wizard-driven	Guided configuration where you can specify video, recording and archiving settings for all your cameras.
General	Specify video, recording and shared settings (such as dynamic archiving paths and whether to record audio or not) for all your cameras.

Camera-specific	Specify video, recording and camera-specific settings (such as event notification, PTZ preset positions and fisheye view areas) for each individual camera.

About database resizing

In case recordings for a camera get bigger than expected, or the available drive space is suddenly reduced in another way, an advanced database resizing procedure automatically takes place:

- If archives (see "About archiving" on page 126) are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive is moved to another drive (moving archives is only possible if you use dynamic archiving (see "Dynamic path selection (properties)" on page 73), with which you can archive to several different drives) or—if moving is not possible—deleted.
- If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive is reduced by deleting a percentage of their oldest recordings, temporarily limiting the size of all databases.

When the Recording Server service (see "About services" on page 169) is restarted upon such database resizing, the original database sizes are used. Therefore, you should make sure to solve the drive size problem. Should the database resizing procedure take place, you are informed on-screen in XProtect Smart Client, in log files, and, if set up, through notifications.

About motion detection

Motion detection settings are linked to the Recording properties settings for the camera under which you can enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your system: your motion detection configuration determines when the system generates motion events and typically also when video is recorded.

Motion detection is enabled as default. Disabling it improves the CPU and RAM performance of your system, but can also affect your motion detection, event and alarm management.

Time spent on finding the best possible motion detection configuration for each camera helps you avoid unnecessary recordings. Depending on the physical location of the camera, it may be a good idea to test motion detection settings under different physical conditions such as day/night and windy/calm weather.

Before you configure motion detection for a camera, Milestone recommends that you have configured the camera's image quality settings, for example resolution, video codec and stream settings. If you later change image quality settings, you should always test any motion detection configuration afterwards.

In the following two tables, you can see the differences between enabling (table 1) and disabling (table 2) built-in motion detection for a camera.

Enabled motion detection

Recording properties setting	Recordings	Motion-based events	Non-motion based events	Sequences
Always	Yes	Yes	Yes	Yes
Never	No	Yes	Yes	No
Built-in Motion Detection	Yes	Yes	Yes	Yes
Built-in Motion Detection & Event or Event only	Yes	Yes	Yes	Yes

Disabled motion detection

Camera's recording settings	Recordings	Motion-based events	Non-motion based events	Sequences
Always	Yes	No	Yes	No
Never	No	No	Yes	No
Built-in Motion Detection	No	No	Yes	No
Built-in Motion Detection and Event or Event only	Yes (depending on settings)	No	Yes (depending on settings)	No

Motion detection sensitivity

Motion detection is per default set up for dynamic sensitivity. However, you can also adjust the sensitivity level manually under **Motion Detection** properties.

Milestone recommends that you do not enable manual sensitivity because:

- With dynamic sensitivity, the system calculates and optimizes the sensitivity level automatically and suppresses the motion detections that come from noise in the images.
- Dynamic sensitivity improves motion detection at nighttime, where the noise in the images often triggers false motion.
- The system is not overloaded from too much recording.
- The users are not missing results from too little recording.

Motion detection and PTZ cameras

Motion detection generally works the same way for pan-tilt-zoom (PTZ) cameras as it does for regular cameras. However, you cannot configure motion detection separately for each of a PTZ camera's preset positions.

About motion detection and PTZ cameras

Motion detection generally works the same way for pan-tilt-zoom (PTZ) cameras as it does for regular cameras. However, you cannot configure motion detection separately for each of a PTZ camera's preset positions.

In order to activate unwanted recordings, notifications and more, the system automatically disables motion detection while a PTZ camera moves between two preset positions. After a number of seconds has passed, the system automatically enables motion detection again. This period of time is known as the transition time and is specified on the PTZ camera's PTZ patrolling properties (see "PTZ patrolling" on page 103).

Configure camera-specific schedules

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

Use the **Configure events** list, located below the other fields to define events that suit your needs.

The fact that a camera transfers video to your system does not necessarily mean that video from the camera is recorded. Recording is configured separately, see Configure video and recording (see "About video and recording configuration" on page 64).

For each camera, you can create schedule profiles based on:

Properties available in all XProtect software versions:

Online periods

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:
- Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow:

  The two options can be combined , but they cannot overlap in time.

Speedup

- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green:

E-mail notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in blue:

PTZ patrolling

- Periods of time (example: Mondays from 08.30 until 17.45), shown in red:
- If use of one patrolling profile is followed immediately by use of another, run your mouse pointer over the red bar to see which patrolling profile applies when.

Properties available in XProtect Enterprise and XProtect Professional only:

SMS notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in green:

Set up a profile

1. In the **Schedule Profiles** list, select **Add new...**.
2. In the **Add Profile** dialog, enter a name for the profile. Names must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
3. In the top right corner of the dialog, select **Set camera to start/stop on time** to base subsequent settings on periods of time or **Set camera to start/stop on event** to base subsequent settings on events within periods of time.
4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.
    - You specify each day separately.
    - You specify time in increments of five minutes. XProtect Professional helps you by showing the time over which your mouse pointer is positioned.

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

- Use the **Configure events** list, located below the other fields to define events that suit your needs.
- To delete an unwanted part of a schedule profile, right-click it and select **Delete**.
- To quickly fill or clear an entire day, double-click the name of the day.
- As an alternative to dragging inside the calendar section, use the **Start time**, **End time** and **Day** fields, then the **Change Period** or **Set Period** button as required. When using the **Start time** and **End time** fields, remember that time is specified in increments of five

minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

Configure when cameras should do what

Use the scheduling feature to configure when:

- Cameras should be online and transfer video to your system.
- Cameras should use speedup to use a higher than normal frame rate
- You want to receive email and/or SMS notifications regarding cameras
- PTZ cameras should patrol, and according to which patrolling profile
- Archiving should take place

See Configure general scheduling and archiving (on page 131) and Configure camera-specific schedules (on page 67).

Configure motion detection

To configure motion detection, do the following:

1. Expand **Advanced Configuration** > **Cameras and Storage Information**, right-click the relevant camera > **Properties**.
2. In the **Camera Properties** window, select the **Recording Properties** tab > select the relevant settings (see "About motion detection" on page 65).
3. Select the **Motion Detection** tab. If there are any areas to exclude from motion detection (for example, if the camera covers an area where a tree is swaying in the wind), you can exclude that area (see "Adjust motion detection: Exclude regions" on page 53) by selecting it with your mouse.
4. Fill in the relevant properties (see "Motion detection & exclude regions" on page 96). Note that there are some differences in motion-detection behavior for PTZ cameras (see "About motion detection and PTZ cameras" on page 67).

Disable or delete cameras

All cameras are enabled by default. This means that video from the cameras can be transferred to your system if the cameras are scheduled to be online (see "Online period" on page 134).

To **disable** a camera:

1. Expand **Advanced Configuration**, expand **Cameras and Storage Information**, double-click the camera you want to disable, and clear the **Enabled** box.
2. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

To **delete** a camera, you have to delete the hardware device (see "Delete hardware devices" on page 59). If you delete the hardware device, you also delete any attached microphones or speakers. If you do not want this, consider disabling the camera instead.

Move PTZ type 1 and 3 to required positions

For PTZ types 1 and 3, you can move the PTZ camera to required positions in several different ways:

1. Click the required position in the camera preview (if supported by the camera).
2. Use the sliders located near the camera preview to move the PTZ camera along each of its axes: the X-axis (for panning left/right), the Y-axis (for tilting up/down), and the Z-axis (for zooming in and out; to zoom in, move the slider towards **Tele;** to zoom out, move the slider towards **Wide**).
3. Use the navigation buttons:

Moves the PTZ camera up and to the left

Moves the PTZ camera up

Moves the PTZ camera up and to the right

Moves the PTZ camera to the left

Moves the PTZ camera to its home position (that is default position)

Moves the PTZ camera to the right

Moves the PTZ camera down and to the left

Moves the PTZ camera down

Moves the PTZ camera down and to the right

Zooms out (one zoom level per click)

Zooms in (one zoom level per click)

Recording and storage properties

Recording and archiving paths (properties)

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

You can edit all properties on a white background. You cannot edit properties on a light blue background. Note that all of the properties can also be specified individually for each camera.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Shortcut	Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.

Name	Description
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 126). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention time	Total amount of time for which you want to keep recordings from the camera (that is, recordings in the camera's database as well as any archived recordings). Default is 7 days. Retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Dynamic path selection (properties)

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. In the case of dynamic path selection, this is because the properties are shared by all cameras.

With dynamic archiving (see "About archiving" on page 126) paths, you specify a number of different archiving paths, usually across several drives. If the path containing the system database is on one of the drives you have selected for archiving, the system always tries to archive to that drive first. If not, the system automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact has no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras. You cannot configure dynamic archiving paths for individual cameras.

Name	Description
Enable dynamic path selection archives	Enables the use of dynamic path selection, allowing you to select which paths you want to use. The list of selectable paths initially represents all drives on the server, both local and mapped drives. You can add further paths with the **New path** feature below the list.
Use	Select particular paths for use as dynamic archiving paths. You can also select a previously manually added path for removal (see description of **Remove** button in the following).
Drive	Letter representing the drive in question, for example C:.
Path	Path to where you save the files, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
Drive Size	Total size of the drive.
Free Space	Amount of unused space left on the drive.
New path	Specify a new path, and add it to the list using the Add button. Paths must be reachable by the surveillance system server, and you must specify the path using the UNC (Universal Naming Convention) format, example: \\server\volume\directory\. When the new path is added, you can select it for use as a dynamic archiving path.
Add	Add the path specified in the **New path** field to the list.
Remove	Remove a selected path—which has previously been manually added—from the list. You cannot remove any of the initially listed paths, not even when they are selected.

Video recording (properties)

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. Either in order to speed up things, or

because the properties in question are shared by all cameras rather than being specific to individual cameras.

The term **recording** means saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

You can edit all properties on a white background. You cannot edit properties on a light blue background. Note that you can also specify all of the Video Recording properties individually for each camera (see "Recording" on page 91).

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Name	Description
Record on	Select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 86) and scheduled to be online (see "Online period" on page 134) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 96) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. Use the **Configure events** list, located below the other fields to define events that suit your needs. • **Motion Detection and Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 126) times. That can be problematic since pre-recording does not work well during archiving.

Name	Description
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

If the camera uses the MJPEG video format

With MJPEG, you can define frame rates for regular as well as speedup modes. If the camera offers dual stream, you can also enable this.

Note that there are three places where you can set frame rate:

- Live Frame Rate - used for the regular recording stream
- Live Frame Rate - used when speeding up recordings in connection with motion detection or similar functionality.
- FPS (Frames per second) - used for the additional stream used for live viewing.

Regular frame rate mode:

Properties available for all XProtect software versions:

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).

Properties available in XProtect Enterprise and XProtect Professional only:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Speedup frame rate mode:

Properties available in all XProtect software versions:

Name	Description
Enable speedup frame rate	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
On motion	Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.
On event	Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists. Use the **Configure events** list, located below the other fields to define events that suit your needs.
Start Event	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.

Properties available in XProtect Enterprise and XProtect Professional only:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.

Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Tip: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling (see "Speedup" on page 135) to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

If the camera uses the MPEG video format

With MPEG, you can define frame rate and other settings:

Properties available in all XProtect software versions:

Name	Description
Frame rate per second	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

Properties available in XProtect Enterprise, XProtect Professional and XProtect Express only:

Record keyframes only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reducing the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur.
Record all frames on motion	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when motion is detected. Two seconds after the last motion **is detected**, the camera will return to recording keyframes only**.**

Record all frames on event	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists. Use the **Configure events** list, located below the other fields to define events that suit your needs.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Manual recording

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. In the case of manual recording, it is because the properties are shared by all cameras.

When manual recording is enabled, XProtect Smart Client users with the necessary rights can manually start recording if they see something of interest while viewing live video from a camera which is not already recording.

If enabled, manual recording can take place even if recording for individual cameras (see "Recording" on page 91) is set to **Never** or **Conditionally**.

When started from XProtect Smart Client, such user-driven recording always takes place for a fixed time, for example for five minutes.

Name	Description
Enable manual recording	Select check box to enable manual recording and specify further details.
Default duration of manual recording	Period of time (in seconds) during which user-driven recording take place. Default duration is 300 seconds, corresponding to five minutes.
Maximum duration of manual recording	Maximum allowed period of time for user-driven recording. This maximum is not relevant in connection with manual recording started from the Smart Client, since such manual recording will always take place for a fixed time. In some installations it is, however, also possible to combine manual recording with third-party applications if integrating these with XProtect Professional through an API or similar, and in such cases specifying a maximum duration may be relevant. If you are simply using manual recording in connection with the Smart Client, disregard this property.

Frame rate - MJPEG

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

You can edit all properties on a white background. You cannot edit properties on a light blue background. Note that all of the Frame rate - MJPEG properties can also be specified individually for each camera (see "Recording" on page 91) using MJPEG.

Template and common properties

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Name	Description
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Regular frame rate properties

Properties available in all XProtect software versions:

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Time Unit	Select required unit for live and recording frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per **second** in normal mode, you cannot specify 16 frames per **minute** or **hour** in speedup mode.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

Properties available in XProtect Enterprise and XProtect Professional only:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Speedup frame rate properties

Properties available in all XProtect software versions:

Name	Description
Enable Speedup	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.

Name	Description
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Time Unit	Select required unit for live and recording frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per **second** in normal mode, you cannot specify 16 frames per **minute** or **hour** in speedup mode.
Speedup On	• **Motion Detection**: Select this to speed up when motion (see "Motion detection & exclude regions" on page 96) is detected. Normal frame rates will be resumed immediately after the last motion **is detected.** • **Event:** Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring columns. Use the **Configure events** list, located below the other fields to define events that suit your needs. • **Motion Detection & Event:** Select this to speed up when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Schedule Only	Select this to speed up according to the camera's speedup schedule (see "Speedup" on page 135) only.
Start Event	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

Properties available in all XProtect software versions:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.

Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Frame Rate - MPEG

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

Note that you can also specify all of the Frame Rate - MPEG properties individually for each camera (see "Recording" on page 91) using MPEG.

Properties available in all XProtect software versions:

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Dual Stream	Allows you to check if dual streaming is enabled on the camera(s). Note that the information is read-only. For cameras that support dual streaming, this can be enabled/disabled as part of individual cameras' Video (on page 87) properties.
Live FPS	Select the camera's live frame rate per second (FPS).
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Properties available in XProtect Enterprise and XProtect Professional only:

Record Keyframe Only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change; this helps greatly reduce the size of MPEG files. Select the check box if you only want to record keyframes.
Record All Frames on	Allows you to make exceptions if you have selected to record keyframes only. • **Motion Detection**: Select this to record all frames when motion is detected. Two seconds after the last motion (see "Motion detection & exclude regions" on page 96) is detected, the camera will return to recording keyframes only**.** • **Event**: Select this to record all frames when an event occurs and until another event occurs. Requires that events have been defined, and that you select start and stop events in the neighboring columns. Use the **Configure events** list, located below the other fields to define events that suit your needs. • **Motion Detection & Event**: Select this to record all frames when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns. • **Schedule only**: Select this to record all frames according to the camera's speedup schedule (see "Speedup" on page 135) only.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Audio recording

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you can determine whether audio should be recorded or not. Your choice applies for all cameras on your system.

Name	Description
Always	Always record audio on all applicable cameras.
Never	Never record audio on any cameras. Note that even though audio is never recorded, it is still be possible to listen to live audio in the Smart Client.

If you record audio, it is important that you note the following:

- Audio recording affects video storage capacity: Audio is recorded to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since your system automatically archives (see "About archiving" on page 126) data if the database becomes full. However, you may need additional archiving space if you record audio.
    - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) are stored in one record in the database. Each second of audio will also be stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
    - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

Above examples are simplified. The exact available video storage capacity also depends on GOP/JPEG and audio kilobyte size.

Audio selection

When you configure video and recording (see "About video and recording configuration" on page 64), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras. With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker is automatically used when you view video from the camera. Note that all of the properties can also be specified individually for each camera.

Properties available in all XProtect software versions:

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Default Microphone	Select a default microphone.

Name	Description
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
Set all template values on selected cameras	Apply all values from the template to selected cameras.
Properties available in XProtect Enterprise and XProtect Professional only:	
Default Speaker	Select a default speaker.

Storage information

The storage information properties show how much storage space you have on your system and how much of it is free. To quickly view disk space usage in a pie chart format, select the line representing the drive you are interested in.

Name	Description
Drive	Letter representing the drive in question, for example C:.
Path	Path to where you save the files, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
Usage	What the storage area is used for, for example recording or archiving.
Drive Size	Total size of the drive.
Video Data	Amount of video data on the drive.
Other Data	Amount of other data on the drive.
Free Space	Amount of unused space left on the drive.

Camera properties

General

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, properties include:

Name	Description
Enabled	Cameras are by default enabled, meaning that provided they are scheduled to be online (see "Online period" on page 134) and that they can to transfer video to XProtect Professional. You can disable an individual camera, in which case no video/audio is transferred from the camera source to your system.
Preview	Select this check box to show a preview of your camera's video. If you clear the check box, your system does not show a preview for your camera.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Camera shortcut number	Users of XProtect Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for XProtect Smart Client.

These properties are to a large extent camera-specific. Since such properties vary from camera to camera, descriptions in the following are for guidance only. If you can access the selected camera, a live preview is displayed. Click the **Camera Settings...** button to open a separate window with properties for the selected camera.

The video properties typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, and more by overwriting existing values of selecting new ones. When you adjust video settings, you can—for most cameras—preview the effect of your settings in an image below the fields.

Video settings may feature an **Include Date and Time** setting. If set to **Yes**, date and time from the camera are included in video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by your system upon reception, and exact date and time information for each image is already known, it is recommended that the setting is set to **No**.

For consistent time synchronization, you may—if supported by the camera—automatically synchronize camera and system time through a time server.

Video

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you can use either the MJPEG video format or the MPEG video format. Depending on which of the two options, you choose, you can set different options for your camera.

MJPEG video format

With MJPEG, you can define frame rates for regular as well as speedup modes. If the camera offers dual stream, you can also enable this. Note that there are three places where you can set frame rate:

- Live Frame Rate - used for the regular recording stream
- Live Frame Rate - used when speeding up recordings in connection with motion detection or similar functionality.
- FPS (Frames per second) - used for the additional stream used for live viewing.

Regular frame rate mode

Properties available for all XProtect software versions:

Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).

Properties available in XProtect Enterprise and XProtect Professional only:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Speedup frame rate mode

Properties available in all XProtect software versions:

Enable speedup frame rate	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
On motion	Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.
On event	Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists.

Start Event	Select required start event. The camera begins using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera returns to the normal frame rates when the stop event occurs.

Properties available in XProtect Enterprise and XProtect Professional only:

Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Note: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream

Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

MPEG video format

With MPEG, you can define frame rate and other settings:

Frame rate

Properties available in all XProtect software versions:

Frame rate per second	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

Properties available in XProtect Enterprise, XProtect Professional and XProtect Express only:

Record keyframes only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reducing the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur.
Record all frames on motion	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when motion is detected. Two seconds after the last motion **is detected**, the camera will return to recording keyframes only**.**
Record all frames on event	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera begins recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera only records keyframes when the stop event occurs.

Dual stream

Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Audio

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, properties include the possibility of selecting a default microphone and/or speaker for the camera. With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker is automatically used when you view video from the camera.

If a microphone/speaker is attached to the same hardware device as the camera, that particular microphone/speaker is the camera's default microphone/speaker if you do not select otherwise.

Properties available in all XProtect software versions:

Name	Description
Default Microphone	Select a default microphone.

Properties available in XProtect Enterprise and XProtect Professional only:

Default Speaker	Select a default speaker.

The ability to select a default microphone or speaker for the camera is only available if at least one microphone and/or speaker has been attached to a hardware device on the surveillance system.

Recording

The term **recording** means **saving video** and, if applicable, **audio** from a camera in the camera's database on the surveillance system server. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, recording properties include:

Name	Description
Always	Record whenever the camera is enabled (see "General" on page 86) and scheduled to be online (see "Online period" on page 134) (the latter allows for time-based recording).
Never	Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
Conditionally	Record when certain conditions are met. When you select this option, specify required conditions (see the following) which enables you to store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. Say you have specified that video should be stored conditionally on event, with a start event called **Door Opened** and a stop event called **Door Closed**. With three seconds of pre-recording, video is recorded from three seconds before **Door Opened** occurs and until **Door Closed** occurs.
Built-in motion detection	Select this check box to record video in which motion (see "Motion detection & exclude regions" on page 96) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
On event	Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring lists. Use the **Configure events** list, located below the other fields to define events that suit your needs.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

Name	Description
Enable pre-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
Enable post-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.

Note that manual recording (on page 79) may be enabled. With manual recording, users of XProtect Smart Client with the necessary rights can manually start recording if they see something of interest while viewing live video from a camera which is not already recording. If enabled, manual recording can take place even if recording for individual cameras is set to **Never** or **Conditionally**.

Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, properties include:

Component	Requirement
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Delete Database	Click button to delete all recordings in the database for the camera. Archived recordings will not be affected. **IMPORTANT:** Use with caution. All recordings in the database for the camera will be permanently deleted. As a security measure, you are asked to confirm the deletion.

Component	Requirement
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 126). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Delete Archives	Click button to delete all archived recordings for the camera. Recordings in the camera's regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths. **IMPORTANT:** Use with caution. All archived recordings for the camera are permanently deleted. As a security measure, you are asked to confirm the deletion.
Retention time	Total amount of time for which you want to keep recordings from the camera (that is, recordings in the camera's database as well as any archived recordings). Default is 7 days. Retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.

Component	Requirement
Database Repair Action	Select which action to take if the database becomes corrupted: ▸ **Repair, scan, delete if fails**: Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted. ▸ **Repair, delete if fails**: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted. ▸ **Repair, archive if fails**: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived. ▸ **Delete (no repair)**: If the database becomes corrupted, the contents of the database will be deleted. ▸ **Archive (no repair)**: If the database becomes corrupted, the contents of the database will be archived. If you choose an action to repair a corrupt database, this corrupt database is closed while it is repaired. Instead, a new database is created to allow recordings to continue. XProtect Smart Client can often repair a corrupt database if it has been archived. When you open the corrupt database in XProtect Smart Client, XProtect Smart Client repairs the database automatically if at all possible. **Tip:** There are several things you can do to prevent (see "About protecting recording databases from corruption" on page 34) that your databases become corrupt in the first place.
Configure Dynamic Paths	With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the drive containing the camera's database is among the path you have selected for dynamic archiving, XProtect Professional always tries to archive to that path first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. See also Dynamic path selection (see "Dynamic path selection (properties)" on page 73).

Event notification

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, properties include event notification. Event notifications inform XProtect Smart Client users that an event has occurred on your system. Event notifications can be valuable for client users, as they can quickly detect that an event has occurred. Even though you configure event notifications separately for each camera, you can select between all events on your system, regardless whether events are manual, generic or originate on another hardware device than the camera itself.

In the XProtect Smart Client, event notification is given by a yellow indicator which lights up when a relevant event has taken place. You can also add an optional sound on event notification in XProtect Smart Client itself.

Three indicators are available for each camera in XProtect Smart Client:

- The yellow event indicator. Lights up when a relevant event has taken place.
- A red motion indicator. Lights up when motion has been detected.
- An optional green video indicator. Lights up when video is received from the camera.

You can turn off the bar in which the indicators are displayed in XProtect Smart Client. Do not turn off if XProtect Smart Client must rely on event notifications.

Select required events

1. In the **Available events** list, select the relevant event. You can only select one event at a time.
2. Click the **>>** button to copy the selected event to the **Selected Events** list.
3. Repeat for each required event.

If you later want to remove an event from the **Selected Events** list, select the relevant event, and click the **<<** button.

Output

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you can also associate a camera with particular hardware output (see "Add a hardware output" on page 111), for example the sounding of a siren or the switching on of lights.

Associated output can then be activated automatically when motion is detected in video from the camera, or manually when Smart Client users with the necessary rights (see "Configure user and group rights" on page 165) view live video from the camera.

1. In the **Available output** list, select the required output. It is only possible to select one output at a time. If you have not yet defined any suitable output, you can quickly do it: Use the **Configure Output** button, located below the other fields.
2. Click the **>>** button to copy the selected output to the:

- **On manual activation** list, in which case the output is available for manual activation in XProtect Smart Client.

  and/or

- **On motion detected** list, in which case the output is activated when motion is detected in video from the camera. If required, the same output can appear on both lists.

3. Repeat for each required output.

If you later want to remove an output from the one of the lists, select the output in question, and click the **<<** button.

Motion detection & exclude regions

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, adjusting motion detection is important because it may determine when video from the camera is recorded, when e-mail notifications are generated or when hardware output (such as lights or sirens) is activated. Time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary recordings and notifications. Depending on the physical location of the camera, it may be a very good idea to test motion detection under different physical conditions such as day/night or windy/calm weather.

Before you configure motion detection for a camera, you should configure the camera's video properties (see "General" on page 86), such as compression, resolution and more.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

Name	Description
Enable	Enable or disable (see "About motion detection" on page 65) the built-in motion detection.
Show grid	Turn the grid on and off. Turning the grid off may provide a less obscured view of the preview image. You select the areas to exclude from motion detection the same way as when the grid is visible. When the grid is turned on, the preview image is divided into small sections by a grid. To define areas which should be excluded from motion detection, drag the mouse over the areas in the preview image while pressing the mouse button down. The left mouse button selects a grid section and the right mouse button clears a grid section. Selected areas are highlighted in blue.
Include All	Quickly select all grid sections in the preview image. This can be useful if you want to exclude motion detection in most areas of the image, in which case you can clear the few sections in which you do not want to exclude motion detection.
Exclude All	Clear all grid sections in the preview image.

Name	Description
Manual sensitivity	Enable this functionality to be able to adjust the Sensitivity slide for motion yourself. Drag the slider to the left for a higher sensitivity level, and to the right for a lower sensitivity level. ▸ The **higher** the sensitivity level, the less change is allowed in each pixel before it is regarded as motion. ▸ The **lower** the sensitivity level, the more change in each pixel is allowed before it is regarded as motion. Pixels in which motion is detected are highlighted in green in the preview image. Milestone recommends that you do not enable manual sensitivity because: ▸ With dynamic sensitivity, the system calculates and optimizes the sensitivity level automatically and suppresses the motion detections that come from noise in the images. ▸ Dynamic sensitivity improves motion detection at nighttime, where the noise in the images often triggers false motion. ▸ The system is not overloaded from too much recording. ▸ The users are not missing results from too little recording.
Sensitivity	Use this to determine how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. Areas in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted. The more you drag the slider to the left, the more of the preview image becomes highlighted. This is because with a high sensitivity even the slightest change in a pixel will be regarded as motion. As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting.

Name	Description
Motion	Adjust the **Motion** slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the **Level** bar above the sliders. The black vertical line serves as a threshold. When motion is above (to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection. Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting. The more you drag the slider to the left, the more positive motion detections you see because less change will be needed to trigger a positive motion detection. The number of positive motion detections may also affect the amount of video you record, the amount of notifications you receive and more.
Keyframe Only	Select **Keyframe only** if you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection.
Detection interval	Specify how often motion detection analysis is carried out on video from the camera. The default is every 240 milliseconds (close to once a quarter of a second). The interval is applied regardless of your cameras' frame rate settings. Adjusting this setting can help lower the amount of system resources used on motion detection.
Detection resolution	Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.

Privacy masking

If you need to mask any areas of the camera image from viewing, set the following properties:

Name	Description
Enable	Enable the **Privacy Masking** feature.
Show grid	Turn the grid on or off. Turning the grid off may provide a less obscured view of the preview image. Select areas to exclude the same way as you would when the grid is visible. When on, the preview image is divided into small sections by a grid. To define areas which should be excluded from privacy masking, drag the mouse over the areas in the preview image while pressing the mouse button down. The left mouse button selects a grid section and the right mouse button clears a grid section. Selected areas are highlighted in red.

Name	Description
Show privacy mask	Turn the red area indicating privacy masking on or off. Turning off the red area may provide a less obscured view of the preview image.
Clear	Clear the privacy masking.

360° lens

360° lens technology allows you to view 360° panoramic video through an advanced lens. If a camera is going to use 360° lens technology, you must enable the technology and, in some cases, enter a special license key.

Name	Description
Enable 360° lens	Select check box to enable use of the 360° lens technology and to be able to specify further properties.
Enable panomorph support	Select to enable panomorph support. Panomorph is an advanced technology can provide high resolution in zones of interest, while at the same time using fewer pixels than conventional fisheye solutions.
Immervision Enables® panomorph RPL number	When you enable the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list. This is to ensure that the lens is correctly identified and configured with the lens used with the camera. You can usually find the RPL number on the lens itself or on the box it came in. If you, at some point, want to add additional types of lenses, go to **File** and select **Import new lens types.** Locate the .xml file that contains information about the lens type and press **OK.** For details of ImmerVison, panomorph lenses, and RPLs, see http://www.immervision.com/en/home/index.php**.**
Camera position/orientation	Choose whether the camera is mounted in the ceiling, on a wall or on ground level.
Enable fisheye support	Select to enable fisheye support. Fisheye technology uses a wide-angle lens to capture a hemispherical image, which can then be de-warped through configured fisheye settings (see "Fisheye" on page 100) for the camera in question.
License key	If required, enter your special fisheye license key and click OK, after which you can configure fisheye settings for camera(s) attached to the hardware device.

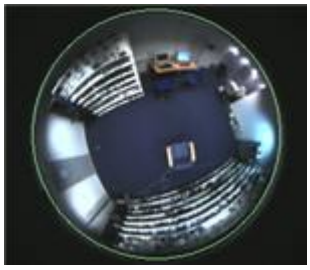
If you are unsure if you need a special fisheye license key, contact your system vendor for further information.

Fisheye

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you may be able to set fisheye properties. Fisheye is a technology that allows you to view 360-degree panoramic video through an advanced lens.

You do not see the fisheye properties until certain conditions are met: the camera must be either a dedicated fisheye camera or be equipped with a special fisheye lens. A special fisheye license key is also required. You enter the key when you configure the hardware device (see "Configure hardware devices" on page 59) to which the fisheye camera is attached.

You configure the camera's fisheye functionality by adjusting its fisheye view field, indicated by a green circle in the fisheye view, until the circle encloses the actual image area of the fisheye lens. Your settings are then used by the fisheye technology for converting the circular fisheye view into a flattened rectangular view.



Name	Description
Ceiling mount	If the camera is mounted on a ceiling, you can adjust properties to reflect this by selecting the check box.
Resolution	Resolution values are automatically displayed above the fisheye image. When using fisheye, resolution will automatically be set to the highest possible value.
X radius	Controls the horizontal (X) radius of the green circle. Move the slider to the left for a narrower circle, or to the right for a wider circle. Alternatively, specify a value between 0 and 800 in the field next to the slider. 0 corresponds to the slider's leftmost position, 800 corresponds to the slider's rightmost position.
Milestone Recording Server service	A vital part of the surveillance system. Video streams are only transferred to your system while the Recording Server service is running.
X center	Controls the horizontal (X) position of the green circle. Move the slider to the left or right as required. Alternatively, specify a value between 0 and 800 in the field next to the slider.
Y center	Controls the vertical (Y) position of the green circle. Move the slider to the left in order to move the circle up, or to the right in order to move the circle down. Alternatively, specify a value between 0 and 800 in the field next to the slider.
Enable preview	Switch between viewing the circular fisheye view and the flattened rectangular view resulting from your settings. When you preview the flattened view, the following navigation buttons become available for moving around within the flattened view.

Name	Description
Set as Home	Use after navigating to a suitable viewpoint using the navigation buttons. Sets the current viewpoint as home position (that is default position), so that when client users viewing the camera click their clients' **Home** button, their view of the camera changes to that position.

Button	Description
	Moves the flattened view up
	Moves the flattened view up and to the left
	Moves the flattened view up and to the right
	Moves the flattened view to the left
	Moves the flattened view to its home position (that is default position)
	Moves the flattened view to the right
	Moves the flattened view down and to the left
	Moves the flattened view down
	Moves the flattened view down and to the right
	Zooms out (one zoom level per click)
	Zooms in (one zoom level per click)

PTZ preset positions

PTZ-related properties are only available when you are dealing with a PTZ (pan-tilt-zoom) camera.

You can use PTZ preset positions for making the PTZ camera automatically go to a particular position when particular events occur, and when setting up PTZ patrolling profiles. Preset positions can also be used in clients to allow users that have been given rights (see "Configure user and group rights" on page 165) to move the PTZ camera between preset positions. Names of preset positions must contain only the characters A-Z, a-z and the digits 0-9. If you import preset positions from cameras (see the

following), verify that their names do not contain other characters. If they do, change the preset position names before you import them.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

Name	Description
PTZ type	Your configuration options depend on the type of PTZ camera in question: • Type 1 (stored on server): You define preset positions by moving the camera using the controls in the upper half of the window, then storing each required position on the system server. You can define up to 50 preset positions this way. • Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used. • Type 3 (stored on camera): You define preset positions by moving the camera with the controls in the upper half of the window, then storing each required position in the camera's own memory. You can define up to 50 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with the system.
Import / Refresh	Only available when you have selected PTZ type 2 or 3. Lets you import already defined preset positions from the camera's memory for use with XProtect Professional. If you have already imported preset positions this way, and preset positions have since then been added or changed on the camera, you can use this button to refresh the imported preset positions.
Add New	Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions. Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.
Set New Position	Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

Name	Description
Delete	Only available when you have selected PTZ type 1 or 3. Lets you delete an already defined preset. In the list, select the preset position you want to delete, then click the button. Before you delete a preset position, make sure it is not used in PTZ patrolling or PTZ on event. Since the preset positions are stored on the camera, you can bring a deleted preset position back into your system by clicking the **Import / refresh** button. If you bring back a preset position this way, and you use the preset position with PTZ patrolling or PTZ on event, you must manually configure the PTZ patrolling and/or PTZ on event to use the preset position again.
Test	Try out a preset position. In the list, select the preset position you want to test, then click the button to view the camera move to the selected position.
PTZ control wheel	Move a preset position selected in the list up and down respectively. The selected preset position is moved one step per click. By moving preset positions up or down, you can control the sequence in which preset positions are presented in clients.

PTZ patrolling

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

You can only set PTZ-related properties for pan-tilt-zoom (PTZ) cameras. PTZ patrolling is the continuous movement of a PTZ camera between a number of preset positions. To use patrolling, you must specify at least two preset positions for the relevant PTZ camera. To configure PTZ patrolling, select a patrolling profile in the **Patrolling profiles** list and specify relevant properties to define the exact behavior of the patrolling profile. When you have defined your patrolling profiles, remember to schedule the use of patrolling profiles. Note that if users manually operate PTZ cameras, this can override patrolling. You can specify a patrolling profile with only one preset if needed. Such a patrolling profile can be useful in two cases: for moving a PTZ camera to a specific position at a specific time, and for moving a PTZ camera to a specific position upon manual control of the PTZ camera.

Patrolling profiles

A PTZ camera may patrol according to several different patrolling profiles. For example, a PTZ camera in a supermarket may patrol according to one patrolling profile during opening hours, and according to another patrolling profile when the supermarket is closed. You can reuse the names of patrolling profiles defined for other cameras. This allows you to use a single patrolling profile name across several PTZ cameras, and can make scheduling of PTZ patrolling much easier. Even though several PTZ cameras share a patrolling profile name, the movement between preset positions is individual for each camera.

From the **Patrolling profiles** list, select which patrolling profile to configure:

Name	Description
Add New	Add a new patrolling profile to the list. When you add a new patrolling profile, you can either give it a unique name, or reuse an existing name from another PTZ camera with PTZ patrolling. Using several identically named patrolling profiles can be advantageous when you later configure scheduling. Example: If you have configured patrolling profiles identically named Night Patrolling on 25 different cameras, you can schedule the use of Night Patrolling on all 25 cameras in one go, even though Night Patrolling covers individual preset positions on each of the 25 cameras.
Delete	Delete an existing patrolling profile. Note that the selected patrolling profile is removed from the list without further warning.

Patrolling list

Having selected a patrolling profile in the **Patrolling profiles** list, you can specify which of the PTZ camera's preset positions to use with the selected patrolling scheme. Use the button to copy a selected preset positions to the **Patrolling list**. To change the sequence of preset positions in the **Preset Positions** list, select a preset position, and use the or buttons to move the selected preset position up or down in the list. The selected preset position is moved one step per click. If you later want to remove a preset position from the Patrolling list, select the preset position in question, and click the button.

Name	Description
Wait time (sec.)	Specify the number of seconds for which the PTZ camera should stay at each preset position before it moves on to the next preset position. The default is 10 seconds. The wait time applies to all presets in the patrolling profile. The PTZ camera stays at each preset position for the same number of seconds.
Transition time (sec.)	Specify the number of seconds needed for the PTZ camera to move from one preset position to another. The default is five seconds. During this transition time, motion detection is automatically disabled, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions. After the specified number of seconds, motion detection is automatically enabled again. The transition time applies to all presets in the patrolling profile. It is important that the camera can switch between any of the patrolling profile's preset positions within the number of seconds you specify. If not, the system is likely to detect false motion. Note that it takes longer for the PTZ camera to move between positions that are located physically far apart (for example from an extreme left position to an extreme right position) than between positions that are located physically close together.

PTZ scanning

PTZ scanning (continuous panning) is supported on a few PTZ cameras only. You can enable PTZ scanning and select a PTZ scanning speed from the list below the check box. PTZ scanning only

works for PTZ type 1 cameras (where preset positions are configured and stored on the server). If the camera is a PTZ type 2 camera, and you import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface, PTZ scanning stops working.

Pause PTZ patrolling

PTZ patrolling pauses automatically when users operate the camera manually as well if your system is using **PTZ on Event**. If the system detects motion, it may also pause PTZ patrolling. Pause settings are tied to the selected patrolling profile. This allows you the flexibility of having different pause settings for different patrolling profiles on the same camera.

Pause patrolling if motion is detected

To pause PTZ patrolling when the system detects motion, so that the PTZ camera remains at the position where the system detected motion for a specified period of time, do the following:

1. Select the **Pause patrolling if motion is detected** check box.
2. Select whether the PTZ camera should resume patrolling:
   - After a certain number of seconds has passed since first detection of motion, regardless whether further motion is detected

     or

   - After a certain number of seconds has passed without further detection of motion
3. Specify the number of seconds for the selected option (default is ten and five seconds respectively).
4. Unless the transition time is set to zero, the system automatically disables motion detection while the camera moves between preset positions, as the system is likely to detect irrelevant motion otherwise while the camera moves between the preset positions.

Resume PTZ patrolling

The system automatically pauses PTZ patrolling when users operate the camera manually as well as if PTZ on Event is in use. You can specify how many seconds should pass before the system resumes regular patrolling after a manual or event-based interruption. The default is 30 seconds.

Apart from manual control, users of XProtect Smart Client can also stop a selected PTZ camera's patrolling entirely. For XProtect Smart Client users, the number of seconds specified in the **Patrolling settings** section therefore only applies when users manually control a PTZ camera and not when users stop a PTZ camera's patrolling entirely. When XProtect Smart Client users stop a PTZ camera's patrolling entirely, the camera's patrolling resumes only when the XProtect Smart Client user selects to resume it.

PTZ on event

PTZ-related properties are only available when you are dealing with a pan-tilt-zoom (PTZ) camera. When a PTZ camera supports preset positions (see "PTZ preset positions" on page 101), you can make the PTZ camera automatically go to a particular preset position when a particular event occurs. When associating events with preset positions on a PTZ camera, you can select between **all** events

defined on your system. You are not limited to selecting events defined on a particular hardware device.

Component	Requirement
Event	Select the relevant event.
PTZ Preset Position	Select the relevant preset position. For this purpose, you can only use an event once per PTZ camera. However, use different events for making the PTZ camera go to the same preset position. Example: ○ Event 1 makes the PTZ camera go to preset position A ○ Event 2 makes the PTZ camera go to preset position B ○ Event 3 makes the PTZ camera go to preset position A

If later you want to end the association between a particular event and a particular preset position, clear the field containing the event. After you have made the PTZ setting changes, restart services (see "Start and stop services" on page 170).

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 170) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 38).

Microphones

About microphones

In your system, **Microphones** are typically attached to hardware devices, and therefore physically located next to cameras. Operators, with the necessary rights, can then listen to recordings through the XProtect Smart Client (provided the computer running the XProtect Smart Client has speakers attached). You manage microphones on your system, meaning you can always manage the microphones attached to cameras, **not** microphones attached to XProtect Smart Client operators' computers.

If you have added more microphones to your system than you need, you can hide the ones you do not need by right-clicking the relevant microphone or speaker and select **Hide**. If you need the hidden microphone again, you can right-click the overall microphone icon and select **Show Hidden Items**.

Configure microphones or speakers

1. Expand **Advanced Configuration > Hardware Devices**, and expand the hardware device to which the relevant microphone or speaker is attached.
2. Right-click the relevant microphone or speaker, and select **Properties**.

3. Specify properties (see "Speaker properties" on page 62) as required.

Configuration of microphones and speakers in your system is very basic. You control volume settings and similar settings on the microphone or speaker units themselves.

Show or hide microphones or speakers

If you have added more microphones or speakers to your system than you need, you can hide the ones you do not need by right-clicking the relevant microphone or speaker and select **Hide**. If you need the hidden microphone/speaker again, you can right-click the overall microphone or speaker icon and select **Show Hidden Items**.

Microphone (properties)

When you configure video and recording (see "About video and recording configuration" on page 64) for specific cameras, you can determine when to record audio. Your choice applies for all cameras on your system.

Microphone properties

Enabled	Microphones are by default enabled, meaning that they can transfer audio to your system. If needed, you can disable an individual microphone, in which case no audio is transferred from the microphone to your system.
Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

On some hardware devices, you can also enable/disable audio on the hardware device itself, typically through the hardware device's own configuration web page. If audio on a hardware device does not work after enabling it in the Management Application, you should verify whether the problem may be due to audio being disabled on the hardware device itself.

Recording settings

Name	Description
Always	Always record audio on all applicable cameras.
Follow video	Record audio only when video is recorded.
Never	Never record audio on any cameras. Note that even though audio is never recorded, it is still be possible to listen to live audio in the Smart Client.

Events and output

About input and output

Hardware input, such as door sensors, can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in your system.

Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from your system. Such hardware output can be activated automatically by events, or manually from clients.

Before you specify use of hardware input and hardware output units on a hardware device, verify the hardware device recognized the sensor operatione. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Professional release notes to verify that the hardware device and firmware used supports input and output-controlled operations.

You do not have to configure hardware input units separately. Any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to your system. The same goes for hardware output, but hardware output does require some simple configuration in your system.

If you want to **configure hardware output** and **automatically trigger output when events occur**, so that, for example, lights are switched on when a door is opened or when motion is detected in video, see Add a hardware output (on page 111) and Configure hardware output on event (on page 113).

About events and output

You can use events and output of various types to automatically trigger actions in your system. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering notifications, making PTZ cameras move to specific preset positions. You can also use events for activating hardware output. You can also configure events and output to generate alarms.

Events can be divided in to:

- **Internal events (system-related):** for example, motion, server responding/not responding, archiving problems and lack of disk space.
- **External events (integrated):** for example, MIP plug-in events.

Overview of events and output

Types of events:

Name	Description
Analytics events:	Analytics events can be used as alarms and integrated seamlessly with the Alarms feature. Analytics events are typically data received from external third-party video content analysis (VCA) providers. An example of a VCA-based system could be an access control system.

Name	Description
Hardware input events:	Hardware input, such as door sensors, can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in XProtect Professional. Events based on input from hardware input units attached to hardware devices are called hardware input events. Some hardware devices have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the hardware devices' own software, typically by accessing a browser-based configuration interface on the hardware device's IP address). When this is the case, XProtect Professional considers such detections as input from the hardware, and you can use such detections as input events as well. Lastly, hardware input events can be based on XProtect Professional detecting motion in video from a camera, based on motion detection settings in XProtect Professional. This type of hardware input events is also called system motion detection events or VMD (Video Motion Detection) events. In earlier XProtect Professional versions, VMD events were an event type of their own. Now, they are considered a type of hardware input event.
Hardware output:	Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from XProtect Professional. Such hardware output can be activated automatically by events, or manually from clients.
Manual events:	Events may be generated manually by the users selecting them in their clients. These events are called manual events. Manual events can be of the type **Global events** or **Timer events:** Global events apply to all hardware whereas timer events are separate events, triggered by the hardware input event, manual event or generic event under which they are defined. Timer events occur a specified number of seconds or minutes after the event, under which they are defined, has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. **Example:** A camera starts recording based on a hardware input event, for example when a door is opened. A timer event stops the recording after 15 seconds.
Generic events:	Input may also be received in the form of TCP or UDP data packages, which can be analyzed by XProtect Professional, and—if they match specified criteria—used to generate events. Such events are called generic events.

Name	Description
Output control on event:	Hardware output can be activated automatically when events occur. For example, when a door is opened (hardware input event), lights are switched on (hardware output). When configuring the output control, you can select between all output and events defined in XProtect Professional. You are not limited to selecting output or events defined on particular hardware devices. You can use a single event for activating more than one output.

Before you configure events of any type, **configure general event handling**, such as which ports XProtect Professional should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes. See Configure general event handling (on page 114).

Before you specify use of hardware input and hardware output units on a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Professional release notes to verify that input and output controlled operations are supported for the hardware device and firmware used.

You do not have to configure hardware input units separately, any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to XProtect Professional. The same goes for hardware output, but hardware output does require some simple configuration in XProtect Professional.

If you want to **configure hardware output** and **automatically trigger output when events occur**, so that, for example, lights are switched on when a door is opened or when motion is detected in video, see Add a hardware output (on page 111) and Configure hardware output on event (on page 113).

When you are ready to **configure events**, see Add a hardware input event (on page 110), Add a generic event (on page 112), and Add a manual event (on page 112). If you want to use timer events with your other events, see Add a timer event (on page 113).

Add an analytics event

To add an analytics event, do the following:

1. Expand **Events and Output**, right-click **Analytics Events** and select **Create New**.
2. Specify required properties (see "Analytics event" on page 117). Click **OK**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a hardware input event

With hardware input events, you can turn input received from input units attached to hardware devices into events in your system.

Before you specify input for a hardware device, verify the hardware device recognizes sensor operation. Most hardware devices can show this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that input-controlled operation is supported for the hardware device and firmware used.

To add and/or configure a hardware input event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Hardware Input Events** and select **Enable New Input Event**.
2. In the **Hardware Input Event Properties** window's list of hardware devices, expand the required hardware device to see a list of pre-defined hardware input.
3. Select the required types of input to use them as events. The types of input often vary from camera to camera. If motion detection (see "Motion detection & exclude regions" on page 96) is enabled in the system for the relevant camera, note the input type **System Motion Detection**, which lets you turn detected motion in the camera's video stream into an event.

   Note that some types of input are mutually exclusive. When you select one type of input, you may therefore note that other types of input become unavailable for selection.
4. For each selected type of input, select required properties (see "Hardware input event" on page 118). When ready, click **OK**, or click the **Add button** to add a timer event (on page 113) to the event you have just created.
5. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a hardware output

With hardware output, you can add external output units, such as lights, sirens and door openers, to your system. Once added, output can be activated automatically by events or detected motion, or manually by client users.

Before you specify output, verify that sensor operation is recognized by the hardware device with which you are going to use the output. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that output-controlled operation is supported for the hardware device and firmware used.

To add a hardware output event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Hardware Output** and select **Add New Output**.
2. In the **Hardware Output Properties** window's list of hardware devices, select the required hardware device, and click the **Add** button below the list.
3. Specify required properties (see "Hardware input event" on page 118).
4. Click **OK**.
5. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

For information about how to configure automatic activation of hardware output when events occur, see Configure hardware output on event (on page 113). You configure output for manual activation in clients as well as for automatic activation on detected motion individually for each camera (see "Output" on page 95).

Add a manual event

With manual events, your users with required rights (see "Configure user and group rights" on page 165) can trigger events manually from their clients. Manual events can be global (shared by all cameras) or tied to a particular camera (only available when the camera is selected). You can use manual events for a wide variety of purposes, for example:

- As start and stop events for use when scheduling cameras' online periods (see "Online period" on page 134). For example, you can make a camera start or stop transferring video to the surveillance system based on a manual event.
- As start and stop events for controlling other camera settings. For example, you can make a camera use a higher frame rate based on a manual event or you can use a manual event for triggering PTZ on event (on page 105).
- For triggering output. Particular output can be associated (see "Configure hardware output on event" on page 113) with manual events.
- For triggering event-based notifications (see "About notifications" on page 144).
- In combinations. For example, a manual event could make a camera start transferring video to the surveillance system while an output is triggered and an e-mail notification is sent to relevant people.

To add a manual event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Manual Events** and select **Add New Manual Event**
2. In the list in the left side of the **Manual Event Properties**, select global or a camera as required.
3. Click the **add** button and specify required properties (see "Hardware input event" on page 118). When ready, click **OK**, or click the **Add** button again to add a timer event (on page 113) to the event you have just created.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a generic event

Your system can analyze received TCP and/or UDP data packages, and automatically trigger events when specified criteria are met. This way, you can easily integrate your surveillance system with a very wide range of external sources, for example access control systems and alarm systems and more. Events based on the analysis of received TCP and/or UDP packets are called generic events.

1. Expand **Advanced Configuration**, then expand **Events and Output**. Right-click **Generic Events** > **Add New Generic Event**.
2. In the **Generic Event Properties** window, click the **Add** button, and specify relevant properties. When ready, click **OK**, or click the **Add** button to add a timer event to the event you have just created.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a timer event

Timer events are separate events, triggered by the type of event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:

- A camera starts recording based on a hardware input event, for example when a door is opened. A timer event stops the recording after 15 seconds
- Lights are switched on and a camera starts recording based on a manual event. A timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

To add a timer event, select any event you have previously configured, click the **Add** button, and specify required properties (see "Timer event" on page 121). Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Tip: You can add as many timer events as required under an event. This way, you can, for example, make one timer event trigger something 10 seconds after the main event, another timer event trigger something else 30 seconds after the main event, and a third timer event trigger something else 2 minutes after the main event.

Configure hardware output on event

Once you have added hardware output (see "Add a hardware output" on page 111), such as lights, sirens, door openers, etc., you can associate the hardware output with events. This way, particular hardware output can be activated automatically when events occur. Example: When a door is opened (hardware input event), lights are switched on (hardware output).

When making the associations, you can select between **all** output and events defined on your XProtect Professional server. You are not limited to selecting output or events defined on particular hardware devices.

1. Expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Output Control on Event** and select **Properties**.
2. Fill in the relevant properties (see "Output control on event (Events and Output-specific properties)" on page 125). Click **OK**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

You can use a single event for activating more than one output. You cannot delete associations, but you can change your selections or select **None** in both columns as required.

Tip: If you have not yet defined any suitable event or output, you can quickly do it: Use the **Configure events** list and/or **Configure Output...** button, located below the list of associations.

Configure general event handling

Before configuring events of any type, configure general event handling, such as which ports XProtect Professional should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes.

1. Expand **Advanced Configuration**, right-click **Events and Output**, and select **Properties.**
2. Specify required properties (see "Ports and polling" on page 116). Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Generate alarms based on analytics events

Generating alarms based on analytics events is normally a three-step process:

1. Enable the analytics events feature and set up its security. A list of allowed addresses can be used to control who can send event data to the system and on which port the server listens.
2. Create the analytics event, possibly with a description of the event, and test it.
3. Use the analytics event as the source of an alarm definition (see "Alarms definition" on page 184).

As indicated, to use VCA-based events (see "VCA" on page 207), most often a third-party VCA tool is required for supplying data to your system. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the applied formatting rules described in the Milestone Analytics Events Developers Manual. Contact Milestone for more details.

Test a generic event

If you have added a generic event, a quick and easy way to test your generic event is to first set up an event notification and then use **Telnet** to send a small amount of data which triggers the generic event and in turn the event notification.

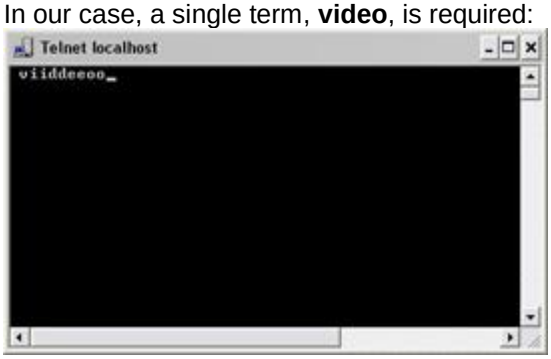
For this example, we have created a generic event called **Video**. Our generic event specifies that if the term **video** appears in a received TCP data package, this should trigger the generic event. Your generic event may be different, but you can still use the principles outlined in the following:

1. In the Management Application navigation pane, expand **Advanced Configurations**, then expand **Cameras and Storage Information**, right-click a camera to which you have access in XProtect Smart Client, and select **Properties**.
2. Select **Event Notification** and select the required generic event. Make sure that your generic event is the **only** event appearing in the **Selected Events** list while you are performing the test, otherwise you cannot be sure that it is your generic event which triggers the event notification. Once you are done testing, you can move any temporarily removed events back to the **Selected Events** list.

3. Save your configuration changes by clicking the **Save Configuration** button in the Management Application toolbar.
4. Make sure the Recording Server service is running. Also make sure that the camera for which you just configured the event notification is displayed and that you have camera title bars enabled in XProtect Smart Client, so you can see the yellow event indicator.
5. In Windows' **Start** menu, select **Run...**, and type the following in the **Open** field:
   - If you are performing the test on the XProtect Professional server itself: `telnet localhost 1234`
   - If you are performing the test from a remote computer: Substitute **localhost** with the IP address of your system's server. Example: If the IP address of the XProtect Professional server is 123.123.123.123, type: `telnet 123.123.123.123 1234`

   This opens a **Telnet** window.

   In the above examples, the number **1234** indicates the port on which the XProtect Professional server listens for generic events. Port 1234 is the default port for this purpose, but you can change this by specifying another port number as part of the general event handling configuration (see "Configure general event handling" on page 114). If you have changed the alert and generic event port number on your system, type your system's alert and generic event port number instead of **1234**.
6. In the **Telnet** window, type the terms (**event substring**) required to trigger your generic event. In our case, a single term, **video**, is required:



   While you type in the Telnet window, you may experience an echo. This is the server repeating some or all of the characters it receives. It will not have any impact as long as you are sure you type the relevant characters.
7. Close the **Telnet** window. You must close the window, since your input is not sent to the surveillance system until you close the window.

8. Go to XProtect Smart Client. If the yellow event indicator lights up for the required camera, your generic event works as intended.:

General event properties

Ports and polling

The **General Event Properties** window lets you specify network settings to be used in connection with event handling.

Name	Description
Alert and generic event port	Specify port number to use for handling events. Default port is port 1234.
SMTP event port	Specify port number to use for sending event information from hardware devices to XProtect Professional via SMTP. Default port is port 25.
FTP event port	Port to use for FTP communication with the hardware device. Default port is port 21.
Polling interval [1/10] second	For a small number of hardware devices, primarily dedicated input/output devices (see "About dedicated input/output devices" on page 58), it is necessary for XProtect Professional to regularly check the state of the hardware devices' input ports in order to detect input. Such state checking at regular intervals is called polling. You can specify (in tenths of a second) the interval between state checks. Default value is 10 tenths of a second (that is one second). For dedicated input/output devices, it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which hardware devices require polling, see the release note.

Events and output properties

Analytics event

When you configure analytics events (see "Add an analytics event" on page 110), specify the following:

Name	Description
Name	Type a name for the event.
Description	Enter a description (optional).
Test Event	Test the validity of the event by clicking this button (optional). **Tip:** You can carry out this test at any step of the analytics event creation/editing process and as many times as you wish.

When you click **Test Event**, a window opens which goes through a number of conditions that must be met for analytics events to work. The window consists of two tabs: **Tasks** and **Errors**.

The **Tasks** tab lists the conditions that are tested and mark them failed: ✗ or success: ✓. The **Errors** tab shows a list of errors corresponding to any failed conditions.

Remember to save any changes made during the test.

When done, check the presence of your test event in the XProtect Smart Client **Alarm list**. Sort by type **Test Alarm** to make your test event appear at the top of the **Alarm list**. See the XProtect Smart Client documentation for more details.

Conditions	Description	Error messages and solutions
Changes saved	If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?	**Save changes before testing analytics event.** Solution/Explanation: Save changes.
Analytics Events enabled	Is the Analytics Event feature enabled?	**Analytics events have not been enabled.** Solution/Explanation: Enable the Analytics Events feature.
Address allowed	Is the IP address/host name of the machine sending the event(s) allowed (listed on the analytics events address list)?	**The local host name must be added as allowed address for the Analytics Event service.** Solution/Explanation: Add your machine to the analytics events address list (of allowed IP addresses/host names). **Error resolving the local host name.** Solution/Explanation: The IP address/host name of the machine cannot be found or is invalid.
Analytics event used in alarm definition	Is the analytics event used actively in any alarm definitions?	**Analytics event is not used in any alarm definition.** Solution/Explanation: Use the analytics event in an alarm definition.

Conditions	Description	Error messages and solutions
Send analytics event	Did sending a test event to the Event Server succeed?	See table below.

Error messages and solutions for the condition **Send analytics event**:

Error messages	Solution/Explanation
Event Server not found.	Unable to find the Event Server service on the list of registered services.
Error connecting to Event Server.	Unable to connect to the Event Server service on the defined port (most likely due to network problems, the Event Server service being stopped or similar).
Error sending analytics event.	Connection to the Event Server service established but event cannot be sent (most likely due to network problems, for example time out).
Error receiving response from Event Server.	Event sent to Event Server but no reply received (most likely due to network problems or port being busy (see the Event Server log, typically located at ProgramData\Milestone\XProtect Event Server\logs\—can be opened in Microsoft Notepad or similar tool)).
Analytics event unknown by Event Server.	The Event Server service does not know the event most likely due to the event, or changes to the event, not having been saved.
Invalid analytics event received by Event Server.	Event format is somehow incorrect.
Sender unauthorized by Event Server.	Most likely your machine is not on the list of allowed IP addresses/host names.
Internal error in Event Server.	An Event Server error. Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Invalid response received from Event Server.	Response is invalid. Possibly due to port being busy or network problems. Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Unknown response from Event Server.	Response is valid but not understood. Possibly due to port being busy or network problems. Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Unexpected error.	Please contact your system provider Milestone Support (support@milestonesys.com) for help.

Hardware input event

When you add hardware input events (see "Add a hardware input event" on page 110), some properties depend on the selected type of input:

Properties available in all XProtect software versions:

Name	Description
Enable	Select check box to use selected type of input as an event in XProtect Professional, and specify further properties.
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Images from camera	Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused the pre- and post-recording feature (see "Recording" on page 91) particular to XProtect Professional. Lets you select which camera you want to receive pre- and/or post-alarm images from.
Number of pre-alarm images	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.
Frames per second	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the Number of pre-alarm images field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.
Delete	Delete a selected event.
Add	When a specific hardware input event is selected, clicking Add adds a timer event (see "Add a timer event" on page 113) to the selected hardware input event.

Properties available in XProtect Enterprise and XProtect Professional only:

Send SMS if this event occurs	Select if the system should automatically send an SMS when the event occurs. You define the recipients of the SMS notifications as part of the SMS notification configuration. When you use SMS notifications, remember that you may have set individual camera scheduling. The setting is only available if you have enabled SMS notifications.

Hardware output

When you add hardware output (see "Add a hardware output" on page 111), specify the following properties:

Name	Description
Output name	Specify a name. If you are going to make the hardware output available for manual activation in clients, this is the name that client users will see. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Output connected to	Select which of the hardware device's output ports the output is connected to. Many hardware devices only have a single output port; in that case simply select **Output 1**.
Keep output for	Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds. Some hardware devices are only able to apply output for a relatively short time, for example for up to five seconds. Refer to the documentation for the hardware device in question for exact information.

To verify that your hardware output works, click the **Test Output** button.

Manual event

When you add manual events (see "Add a manual event" on page 112), specify the following properties:

Properties available in all XProtect software versions:

Name	Description
[List of defined global events and cameras]	Contains a Global node and a list of all defined cameras. You can configure as many manual events as required, no matter whether they are global or camera-specific. A + sign next to the Global node indicates that one or more global manual events have already been configured. A + sign next to a camera indicates that one or more manual events have already been configured for that camera.

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.
Delete	Delete a selected event.
Add	Add a new event. When **Global** or a specific camera is selected, clicking **Add** adds a new manual event. When a specific manual event is selected, clicking **Add** adds a timer event (see "Add a timer event" on page 113) to the selected manual event.
Properties available in XProtect Enterprise and XProtect Professional only:	
Send SMS if this event occurs	Select if the system should automatically send an SMS when the event occurs. You define the recipients of the SMS notifications as part of the SMS notification configuration. When you use SMS notifications, remember that you may have set individual camera scheduling. The setting is only available if you have enabled SMS notifications.

Timer event

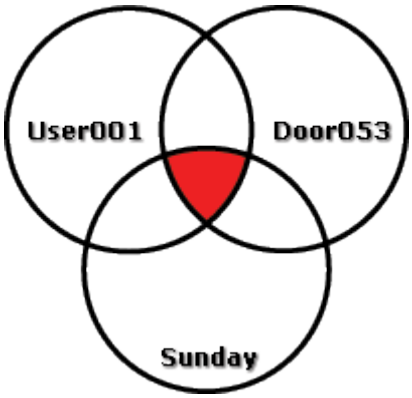
When you add timer events (see "Add a timer event" on page 113), specify the following properties:

Name	Description
Timer event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Timer event occurs after	Specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).

Generic event

When you add generic events (see "Test a generic event" on page 114), specify the following properties:

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Event port	Read-only field displaying the port number on which XProtect Professional listens for generic events (default is port 1234). The port number can be changed as part of the general event handling configuration (see "Configure general event handling" on page 114).
Event substring	Lets you specify the individual items for which XProtect Professional should look out for when analyzing data packages. Specify one or more terms, then click the Add button to add the specified term(s) to the Event message expression field, the content of which will be used for the actual analysis. Examples: • **Single term:** User001 (when added to the Event message expression field, the term will appear as "User001") • **Several terms as one item:** User001 Door053 Sunday (when added to the Event message expression field, the terms will appear as " User001 Door053 Sunday") When you add several terms as one item (appearing as, for example, " User001 Door053 Sunday" in the Event message expression field), everything between the quotation marks must appear together in the package, in the specified sequence, in order to match your criterion. If the terms must appear in the package, but not necessarily in any exact sequence, add the terms one by one (that is so they will appear as "User001" "Door053" "Sunday" in the Event message expression field). **Tip:** It is OK for TCP and UDP packages used for generic events to contain special characters, such as @, #, +, 嶽~, etc. within the text string to be analyzed.

Name	Description
Event message expression	Displays the string which will be used for the actual package analysis. The field is not directly editable. However, you can position the cursor inside the field in order to determine where a new item should be included when you click the Add button or one of the parenthesis or operator buttons described in the following. Likewise, you can position the cursor inside the field in order to determine where an item should be removed when clicking the Remove button: The item immediately to the left of the cursor will be removed when you click the Remove button. • **(:** Lets you add a start parenthesis character to the Event message expression field. Parentheses can be used to ensure that related terms are processed together as a logical unit; in other words, they can be used to force a certain processing order in the analysis. Example: If using ("User001" OR "Door053") AND "Sunday", the two terms inside the parenthesis will be processed first, then the result will be combined with the last part of the string. In other words, XProtect Professional will first look for any packages containing either of the terms User001 or Door053, then it will take the results and run through them in order to see which packages also contain the term Sunday. • **):** Lets you add an end parenthesis character to the Event message expression field. • **AND:** Lets you add an AND operator to the Event message expression field. With an AND operator, you specify that the terms on both sides of the AND operator must be present. Example: If using User001 AND Door053 AND Sunday, the term User001 as well as the term Door053 as well as the term Sunday must be present in order for the criterion to be met. It is not enough for only one or two of the terms to be present. As a rule of thumb, the more terms you combine with AND, the fewer results you will retrieve:  Combinations with AND yields few results (indicated in red) • **OR:** Lets you add an OR operator to the Event message expression field. With an OR operator, you specify that either one or another term must be present. Example: If using User001 OR Door053 OR Sunday, the term User001 or the term Door053 or the term Sunday must be present in order for the criterion to be met. The criterion is satisfied even if only one of the terms is present. As a rule of thumb, the more terms you combine with OR, the more results you will retrieve:

Name	Description
Event priority	The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events. The priority must be specified as a number between 0 (lowest priority) and 1000 (highest priority). When XProtect Professional receives a TCP and/or UDP package, analysis of the packet will start with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority will be triggered. If a package matches the criteria for several events with an identical priority, for example two events with a priority of 999, all events with the priority in question will be triggered.
Event protocol	Select which protocol XProtect Professional should listen for in order to detect the event: • **Any:** Listen for, and analyze, packages using TCP as well as UDP protocol. • **TCP:** Listen for, and analyze, packages using TCP protocol only. • **UDP:** Listen for, and analyze, packages using UDP protocol only.
Event rule type	Select how particular XProtect Professional should be when analyzing received data packages: • **Search:** In order for the event to occur, the received package must contain the message specified in the Event message expression field, but may also have more content. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will be triggered if the received package contains the terms "User001" and "Door053" and "Sunday" since your two required terms are contained in the received package. • **Match:** In order for the event to occur, the received package must contain exactly the message specified in the Event message expression field, and nothing else.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 144) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.

Name	Description
Send SMS if this event occurs	Select if the system should automatically send an SMS when the event occurs. You define the recipients of the SMS notifications as part of the SMS notification configuration. When you use SMS notifications, remember that you may have set individual camera scheduling. The setting is only available if you have enabled SMS notifications.
Delete	Delete a selected event.
Add	Add a new event. When the **Generic Events** node is selected, clicking **Add** will add a new generic event. When a specific generic event is selected, clicking **Add** will add a timer event (on page 113) to the selected generic event.

Output control on event (Events and Output-specific properties)

When you add output controls on events (see "Configure hardware output on event" on page 113), specify the following properties:

Name	Description
Event	Select the required event.
Output	Select the required output event.

Scheduling and archiving

About scheduling

The scheduling feature lets you specify:

- When you want to archive
- That some cameras transfer video to your system at all times
- That some cameras transfer video only within specific periods of time or when specific events occur
- When you want to receive notifications from the system

You can set up general scheduling properties for all your cameras or individual properties per camera. You can set up when:

- One or more cameras should be online and transfer video to your system.
- One of more cameras should use speedup and use a higher than normal frame rate.

- You want to receive any notifications regarding one or more cameras.
- Archiving takes place.
- PTZ cameras should patrol, and according to which patrolling profile

About archiving

Archiving is an integrated and automated feature with which recordings are moved to free up space for new recordings. By default, recordings are stored in the database for each camera. The database for each camera is capable of containing a maximum of 600,000 records or 40 GB. Your system automatically archives recordings if a camera's database becomes full. Consequently, having sufficient archiving space is important.

You do not have to do anything to enable archiving. It runs in the background and is automatically enabled and carried out from the moment your system is installed. The most recent recordings are saved on a local storage in order to prevent network-related problems in the saving process.

The default settings for your system is to perform archiving once a day, or if your database becomes full. You can change the settings for when and how often archiving takes place in the Management Application. You can also schedule archiving up to 24 times a day, with a minimum of one hour between each one. This way, you can proactively archive recordings, so databases never become full. The more you expect to record, the more often you should archive.

You can also change the retention time, which is the total amount of time you want to keep recordings from a camera (recordings in the camera's database as well as any archived recordings) under the properties of the individual camera.

Your system automatically archives recordings if a camera's database becomes full. You only specify **one** time limit (the retention time) as part of the general **Recording and Archiving** paths properties. Note that retention time determines when archiving takes place. Retention time is the total amount of time for which you want to keep recordings from a camera (that is recordings in the camera's database as well as any archived recordings).

Backup of archives

Milestone does recommend that you create backups based on the content of camera databases as it may cause sharing violations or other malfunctions. Instead, create backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could back up the default local archiving directory, **Archives**.

Important: When you schedule a backup, make sure the backup job does not overlap with any scheduled archiving times.

If archiving fails

Under rare circumstances, archiving may fail, for example due to network problems. However, in XProtect Professional this does not pose a threat. XProtect Professional creates a new database and continues archiving in this new database. You can work with and view both this new database and the old one like any other databases.

About archiving locations

The default archiving folder (see "Default File Paths" on page 191) (C:\MediaDatabase) is located on the system server. You can change the default archiving folder to any other location locally, or select a location on a network drive to use as the default archiving folder. In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected.

Because you can keep archives spanning many days of recordings and archiving may take place several times per day, further subfolders, named with the archiving date and time, are also automatically created.

The subfolders are named according to the following structure:

```
...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime
```

If the video encoder does not have several channels, the video encoder channel will always be _1 (example: 00408c51e181_1).

Example: an archiving at 23.15 on 31st December 2012 for a camera with the MAC address 00408c51e181 attached to channel 2 would be stored:

```
C:\MediaDatabase\Archives\00408c51e181_2\2012-12-31-23-15
```

About archiving to other locations

When you archive to other locations than the default archiving directory, your system first temporarily stores the archive in the local default archiving directory, then immediately moves the archive to the archiving location you have specified. Archiving directly to a network drive can mean that archiving time varies depending on the available bandwidth on the network. First storing the archive locally, then moving it speeds up the archiving procedure, and reduces delays in case of network problems.

If you archive to a network drive, the regular camera database can only be stored on a local drive attached directly to your system's server.

About dynamic archive paths

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Milestone recommends using dynamic paths (see "Configure storage wizard" on page 44), which also is the default setting when you configure cameras through the Configure video & recording wizard.

If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, your system always tries to archive to that drive first. If not, your system automatically archives to the archiving drive with the most available space at any time, provided a camera database is not using that drive.

The drive that has the most available space may change during the archiving process, and archiving may happen to several archiving drives during the same process. This does not have impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras. You cannot configure dynamic archiving paths for individual cameras.

When deciding which drives to use for dynamic archiving, consider the pros and cons in the following examples (in which we assume that the default archiving path is on drive C:—drive letters are examples only, different drive letters may of course be used in your organization):

- **Camera records to drive C: and archives to drive C:**

If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, your system tries to archive to that drive first. Archiving takes place quickly, but may also fill up the drive with data fairly quickly.

- **Camera records to drive C: and archives to drive D:**

  Recordings and archives are on separate drives. Archiving takes place less quickly. Your system will first temporarily store the archive in the local default archiving directory on C:, then immediately move the archive to the archiving location on D:. Therefore, you need sufficient space to accommodate the temporary archive on C:.

- **Camera 1 records to drive C: and archives to drive D: while Camera 2 records to drive D: and archives to drive C:**

  Avoid this. One camera's archiving may take up space required for another camera's recordings. In the above example, Camera 1's archiving to D: may result in no recording space for camera 2 on D:. The rule is: "Do not cross recording and archiving drives."•

If you use several surveillance servers in a master/slave setup, each surveillance server must archive to its own mapped location in order for archiving to work. If you attempt to archive to the same mapped location for all the servers, archiving fails.

If you use several surveillance servers in a master/slave setup, each surveillance server must archive to its own mapped location in order for archiving to work. If you attempt to archive to the same mapped location for all the servers, archiving will fail.

About archiving audio

If you have enabled an audio source (for example, a microphone) on a hardware device, audio recordings are archived together with video recordings from the camera attached to the hardware device. If the hardware device is a video encoder with several channels, audio is archived with the camera on channel 1. When you have enabled an audio source, the system records audio to the associated camera's database. This affects the database's capacity for storing video. You may, therefore, want to use scheduled archiving more frequently if you record audio and video than if you only record video.

Storage capacity required for archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to keep, and on how long you want to keep them (retention time). Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.

You should always first consider the storage capacity of the **local** drive containing the default archiving directory to which archived recordings are always moved, even though they may immediately after be moved to an archiving location on another drive. Basically, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

When you archive, XProtect Professional automatically checks that space required for the data to be archived plus 1 GB of free disk space per camera is available at the archiving location. If not, the archive location's oldest data from the camera in question is deleted until there is sufficient free space for the new data to be archived.

When you estimate storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

Tip: The Storage Calculator in the Support section of the Milestone website can help you determine the storage capacity required for your surveillance system.

About archiving schedules

There are two ways in which to configure archiving schedules:

- While you configure your cameras through the Configure Video and Recording wizard (see "Configure storage wizard" on page 44), in which case you configure your archiving schedule on the wizard's **Drive selection** page.
- As part of the general Scheduling and Archiving properties: Expand **Advanced Configuration**, right-click **Scheduling and Archiving**, select **Properties**, select **Archiving** in the dialog, and specify relevant properties (see "Archiving" on page 133).

Automatic response if running out of disk space

If your system runs of disk space while archiving, you can set up an automatic response. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Same drive: Automatic moving or deletion of archives if drive runs out of disk space

If your system server is running out of disk space, and the archiving drive is identical to the camera database drive, your system automatically does a number of attempts to free up space. Most of these attempts will result in the loss of your data from archives or databases.

- First, the system attempts to move archives. You can only move archives if you use dynamic archiving, with which you can archive to several different drives. This happens if:
  - there is less than 15% disk space left, and the available disk space goes below 40 GB plus 2 GB per camera

    - or -
  - the available disk space goes below 225 MB plus 30 MB per camera. Example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 525 MB (225 MB plus 30 MB for each of the ten cameras).

  The difference ensures that very large disks are not necessarily considered to be running out of disk space just because they have less than 15% disk space left.
- If the system cannot move archives, your system attempts to delete the oldest archives. This happens if:
  - there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

  - or -
  - the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks not necessarily are considered to be running out of disk space just because they have less than 10% disk space left.

- If there are no archives to delete, your system attempts to resize camera databases by deleting their oldest recordings. This happens if:
  - there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

  - or -

  - the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

  The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

When the system restarts your recording server after resizing the database, the original databases sizes are used, so you should make sure that the drive size problem is solved or, alternatively, adjust camera database sizes to reflect the altered drive size.

If the system performs the database resizing procedure, you are informed on-screen in XProtect Smart Client, in log files, and or in notifications (if set up).

Different drives: Automatic archiving if database drive runs out of disk space

In case the system server is running out of disk space, and the archiving drive is **different from** the camera database drive, and archiving has not taken place within the last hour, archiving automatically begins in an attempt to free up disk space. This will happen regardless of any archiving schedules. The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

- the available disk space goes below 150 MB plus 20 MB per camera. Example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras).

The difference ensures that very large disks are not necessarily considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, the system automatically checks that the space required for data from a camera to be archived plus 1 GB of free disk space per camera is available. If not, the archive drive's oldest data from the relevant camera is deleted until there is sufficient free space for the new data to be archived.

About viewing archived recordings

You can view archived recordings via XProtect Smart Client. You can, for example, use features such as exporting and browsing with archived recordings.

For archived recordings stored on a local or network drive, you can use XProtect Smart Client's playback features to find and view the relevant recordings, similar to recordings stored in a camera's regular database. You can also use exported archives, archives stored outside local or network drives,

in XProtect Smart Client. For more information, see the XProtect Smart Client documentation at www.milestonesys.com.

Configure general scheduling and archiving

To configure general scheduling and archiving, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration**, right-click **Scheduling and Archiving**, and select **Properties**.
2. Specify properties as required for Scheduling all cameras (on page 131), Scheduling options (on page 133), and Archiving (on page 133).
3. Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

When archiving, disable any virus scanning (see "About virus scanning" on page 12) of camera databases and archiving locations.

General scheduling properties

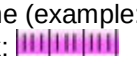
Scheduling all cameras

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 131), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

Note that you can specify the properties for **Online Period**, **Speedup**, **Notifications (Email and SMS)**, and **PTZ Patrolling** individually for each camera.

Properties available for all XProtect software versions:

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera	The name as it appears in the Management Application as well as in clients.

Name	Description
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 67) for the relevant camera(s). You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: The two options can be combined , but they cannot overlap in time.
E-mail	Select the required profile for the e-mail notification schedule for the camera(s) in question. You specify a camera's e-mail notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in blue:
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras.
New schedule profile	Create a new schedule profile of any type by clicking the **Create...** button.

Properties available in XProtect Enterprise and XProtect Professional only:

SMS	Select the required profile for the SMS notification schedule for the camera(s) in question. You specify a camera's SMS notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in green:
PTZ Patrolling	Only available for PTZ (pan-tilt-zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 135) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red:

Scheduling options

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 131), you can specify certain properties for many cameras in one go. In the case of Scheduling Options, it is because the properties are shared by all cameras.

Name	Description
Start cameras on client requests	Cameras may be offline, for example because they have reached the end of an online recording schedule (see "Online period" on page 134), in which case client users will not be able to view live video from the cameras. However, if you select **Start cameras on client requests**, client users will be able to view live video from the camera outside online schedule—but without recording (technically: force the camera to be online outside its online schedule). You must select **Enable recording when started on client request** (see the following), if you want recording to take place.
Enable recording when started on client request	Enable recording on the camera when **Start cameras on client requests** (see the previous) is also selected. If a user does not have access to manual recording (see "Camera access" on page 166), selecting **Enable recording when started on client request**, will **not** enable the user to do manual recording.
Schedule profile for new cameras	Select which online schedule profile to use as default for cameras you subsequently add to your XProtect Professional system. Note that your selection only applies for the online schedule, not for any other schedules. Default selection is **Always on**, meaning that new cameras will always be online, that is transferring video to the XProtect Professional server for live viewing and further processing.
Maximum delay between reconnect attempts	Control the aggressiveness of reconnection attempts. If XProtect Professional loses the connection to a camera, it will by default attempt to re-establish the connection after ten seconds. In some environments, for example if using vehicle-mounted cameras through wireless connections, camera connections may frequently be lost, and you may want to change the aggressiveness of such reconnection attempts.

You can view live and even record video from a camera outside its online recording schedule. To do this, you select the **Start cameras on client requests** and, if needed, the **Enable recording when started on client request** options in the following when setting up your scheduling properties for the camera in question.

Archiving

XProtect Professional automatically archives (see "About archiving" on page 126) recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

Properties available in all XProtect software versions:

Name	Description
Archiving Times	Specify when you want XProtect Professional to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.
Send e-mail on archiving failure	If selected, XProtect Professional will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification feature is enabled. Recipients are defined as part of the e-mail notification properties (see "Email (Properties)" on page 144).
Properties available in XProtect Enterprise and XProtect Professional only:	
Send SMS on archiving failure	Select if the system should automatically send an SMS if archiving fails. You define the recipients of the SMS notifications as part of the SMS notification configuration. The setting is only available if you have enabled SMS notifications.
Properties available in XProtect Enterprise only:	
Archive on event	If selected, your system starts archiving when a certain event occurs. Select the event from the list.

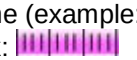
Camera-specific scheduling properties

Online period

When you configure scheduling (see "Configure camera-specific schedules" on page 67) for specific cameras, your **Online Period** settings are probably the most important, since they determine when each camera should transfer video to XProtect Professional.

By default, cameras added to XProtect Professional are automatically online, and you only need to modify the online period settings if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the general scheduling options (see "Scheduling options" on page 133), in which case cameras added at a later time are not automatically online.

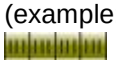
The fact that a camera transfers video to XProtect Professional does not necessarily mean that video from the camera is recorded. Recording is configured separately, see Configure video and recording (see "About video and recording configuration" on page 64).

Name	Description
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 67) for the relevant camera(s). You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: The two options can be combined , but they cannot overlap in time.

Tip: If you want to view live video as well as record video from a camera outside its online recording schedule, you can select the Start cameras on client requests (see "Scheduling options" on page 133) and, if needed, the Enable recording when started on client request **(see "**Scheduling options**" on page 133)** options to set up your scheduling properties for a relevant camera.

Speedup

Speedup may also take place based on events, but that is configured elsewhere. See Frame rate - MJPEG (General recording and storage properties) (see "Frame rate - MJPEG" on page 80) and Video (Camera-specific properties) (see "Video" on page 87).

Name	Description
Speedup	For specific MJPEG cameras, specify speedup periods. Before you can define this type of schedule, you must enable (see "Frame rate - MJPEG" on page 80) speedup. You specify a camera's speedup periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in olive green: 

PTZ patrolling

When you configure scheduling (see "Configure camera-specific schedules" on page 67) for PTZ (pan-tilt-zoom) cameras capable of patrolling (see "PTZ patrolling" on page 103), you can specify which patrolling profiles to use at specific times. Before you can define this type of schedule, you must configure patrolling for the relevant cameras.

Name	Description
PTZ Patrolling	Only available for PTZ (pan-tilt-zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 135) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red:

Use of one patrolling profile may be followed immediately by use of another (example: use the Daytime patrolling profile Mondays from 08.30 until 17.45, then the Evening patrolling profile Mondays from 17.45 until 23.00). Use of two patrolling profiles cannot overlap.

Unlike other types of scheduling, there are no ready-made **Always on** and **Always off** schedule profiles for PTZ patrolling. You can create any number of customized schedule profiles for each camera. When you create a customized schedule profile (see "Configure camera-specific schedules" on page 67) for one camera, you can reuse it with other cameras if required.

Matrix

About Matrix video sharing

The Matrix feature allows distributed viewing of live video from any camera to any Matrix-recipient on a network operating with the system. A computer on you can view which Matrix-triggered video is called a Matrix-recipient. In order to become a Matrix recipient, you must have the XProtect Smart Client installed on the computer.

For more information about Matrix video sharing, refer to the XProtect Smart Client User's Manual, available from www.milestonesys.com, or the XProtect Smart Client's own built-in help system.

There are two ways in which Matrix-triggered video can appear on a Matrix-recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from XProtect Smart Client or from a custom-made website to the relevant Matrix-recipient.
- **Automatic triggering**: Video is sent to the relevant Matrix-recipient automatically when a predefined event occurs, for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.

About Matrix-recipients

A computer on which Matrix-triggered video can be viewed is known as a Matrix-recipient. In order to become a Matrix-recipient, the computer must have the XProtect Smart Client installed.

There are two ways in which Matrix-triggered video can appear on a Matrix-recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from an XProtect Smart Client—or from a custom-made web page—to the required Matrix-recipient.

- **Automatic triggering**: Video is sent to the relevant Matrix-recipient automatically when a predefined event occurs, for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.
- For more information about Matrix-recipients, refer to the XProtect Smart Client User's Manual, available from www.milestonesys.com, or the XProtect Smart Client's own built-in help system.

Configure Matrix

1. Expand **Advanced Configuration**, right-click **Matrix** and select **Properties**.
2. Enable the use of Matrix by selecting the **Enable Matrix** check box.
3. Specify required properties (see "Matrix recipients" on page 137), or, for automatically triggered video sharing, select **Matrix Event Control** and configure Matrix Event Control properties (see "Matrix event control" on page 138). When ready, click **OK.**
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Matrix properties

Matrix recipients

The **Matrix Recipients** tab is used to enable Matrix functionality and to define which computers to display Matrix-triggered live video. A computer on which Matrix-triggered video can be displayed is known as a Matrix-recipient. Being able to view Matrix-triggered video requires that you have installed XProtect Smart Client on the user's computer.

Name	Description
Enable Matrix	Select check box to enable Matrix functionality.
[List of Defined Matrix recipients]	Lists any already defined Matrix recipients, that is computers on which Matrix-triggered video can be displayed. To change the properties of an already defined Matrix recipient, select the required Matrix recipient, make the changes in the fields below the list, then click the Update button. To remove a Matrix recipient from the list, select the unwanted Matrix recipient, then click the **Delete** button.
Name	Name of the Matrix-recipient. Used when you add a new Matrix-recipient or edit the properties of an existing one. The name appears in various day-to-day usage situations. Therefore, is a good idea to use a descriptive and unambiguous name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Address	IP address of the Matrix recipient, used when adding a new Matrix recipient or editing the properties of an existing one.

Name	Description
Port	Specify the port number to be used when sending commands to the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one. The Matrix recipient will listen for commands on this port. By default, port 12345 is used; you can of course specify another port number.
Password	Specify the password to be used when communicating with the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one
Matrix-recipient is an XProtect Smart Client	Select if the relevant Matrix-recipient is an XProtect Smart Client. If you use XProtect Smart Client, distribution of Matrix-triggered live video takes place slightly differently.
Clear	Removes any content in the **Name**, **Address,** and **Password** fields.
Update	Updates the properties of the selected Matrix recipient with the changes made during editing. Available only if you have edited the properties of an existing Matrix recipient.
Add	Adds the new Matrix-recipient to the list. Available only if you have added properties of a new Matrix-recipient in the **Name**, **Address**, **Port**, **Password**, and possibly XProtect Smart Client fields.

Matrix event control

The **Matrix Event Control** tab is used to configure the automatic sending of live video based on predefined events. You can define exactly which events and cameras to use on a per-Matrix recipient basis. The **Matrix Event Control** tab displays the list of Matrix recipients defined on the **Matrix Recipients** tab.

Right-clicking a Matrix recipient brings up a list of devices with belonging events. When you select an event, it will initially be highlighted by a red exclamation mark, indicating that there is additional configuration to be done. Right-clicking an event brings up a list of options for the selected event:

Component	Requirement
Delete [selected event]	Deletes selected event on the selected device.
Connect	Connects to the camera (actual camera is specified after selecting action to be taken).

Component	Requirement
Disconnect, then connect	Disconnect any existing connections, then connect again. With this option the live video will appear in the Matrix recipient on a first-in-first-out basis. Each time a new event occurs, video from the latest event is displayed prominently in a specific position on the Matrix recipient, while at the same time video from the older events is shifted to less prominent positions and eventually ”pushed out” of the Matrix recipient in order to make space for the latest event's video. With the **Connect** option, you may experience that if video triggered by one event on a camera is already shown on the Matrix recipient, videos triggered by another event on the same camera will not be displayed prominently as coming from the latest event – simply because the Matrix recipient is already showing video from the camera in a less prominent position. By selecting **Disconnect, then connect** you can avoid this issue, and ensure that video from the latest event is always displayed prominently.
Disconnect	Disconnects any existing connection. Use if a particular event should cause video to stop being displayed in the Matrix-recipient, even if they are not yet old enough to be “pushed out” of the Matrix-recipient.

If you selected **Connect**, another red exclamation mark will indicate that there is still some configuration to be done. Right-click an action to select which camera to apply the action on.

Alarm Central Display
Motion on [Back Door West Wing] Camera b
Connect
Delete Connect
[Back Door East Wing] Camera a
[Back Door West Wing] Camera b
[Executive Office Cam] Camera 1
[TPIX] Camera 1

In this example, we have specified that when motion is detected on Camera b, the selected Matrix-recipient should connect to Camera b:

Logs

About logs

Your system can generate various logs that shows the activity on system functionality. The following log types are available in your system:

Name	Description
Management Application log files	Shows Management Application activity. For every day you use the Management Application, a new log file is created. You cannot disable this type of logging. Management Application log files are named according to the structure AdminYYYYMMDD.log, for example Admin20091231.log.
Recording Server service log files	Shows Recording Server service activity. A new log file is created for each day this service is used. You cannot disable this type of logging. Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, for example RecordingServer20091231.log.
Image Server service log files	Shows Image Server service activity. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Server service log files are named according to the structure ISLog_YYYYMMDD.log, for example ISLog_20091231.log.
Image Import service log files	Shows Image Import service activity, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only. It enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYMMDD.log, for example ImageImportLog20091231.log.
Event log files	Shows registered events' activity. A new log file is created for each day on which events occur. You cannot disable this type of logging. Event log files should be viewed using XProtect Smart Client (use the **Playback** tab's **Alerts** section).
Audit log files	Shows XProtect Smart Client user activity (if audit logging is enabled). A new log file is created for each day with audit logging enabled and client user activity. Audit log files are named according to the structure is_auditYYYMMDD.log, for example is_audit20091231.log. The _is prefix is due to the fact that the audit log files are generated by the Image Server service.

Log locations

All log files are by default placed in the appropriate **All Users** folder for the operating system you are using. By default, they are stored there for seven days. Note that you can change log file locations as well as the number of days to store the logs when you configure logging.

Log structures

Most log files generated by your system use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

- The header outlines the information contained in the log lines.
- The log lines consist of two main parts: the log information itself as well as an encrypted part. The encrypted part makes it possible, through decryption and comparison, to assert that a log file has not been tampered with.

Log integrity checks

All log files, except Management Application log files, are subjected to an integrity check once every 24 hours. The integrity check is performed by your system's Log Check service. The result of the integrity check is automatically written to a file named according to the structure LogCheck_YYYYMMDD.log, for example LogCheck_20091231.log. Like the log files themselves, the log check files are by default placed in the appropriate **All Users** folder for the operating system you are using.

Any inconsistencies are reported in the form of error messages written in the log check file.

Possible error messages:

Name	Description
Log integrity information was not found. Log integrity can't be guaranteed.	The log file could not be checked for integrity.
Log information does not match integrity information. Log integrity can't be guaranteed.	The log file exists, but does not contain the expected information. Log integrity cannot be guaranteed.
[Log file name] not found	The log file was not present.
[Log file name] is empty	The log file was present, but empty.
Last line changed/removed in [log file name]	The last line of the log file did not match the validation criteria.
Encrypted data missing in [log file name] near line [#]	The encrypted part of the relevant log line was not present.
Inconsistency found in [log file name] near line [#]	The log line does not match the encrypted part.
Inconsistency found in [log file name] at beginning of log file	The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

Note: Other messages that are not error-related may also appear in the log check file.

Configure system, event and audit logging

XProtect Professional can generate various logs.

To configure logging, do the following:

1. Expand **Advanced Configuration**, right-click **Logs** and select **Properties**.
2. Specify properties (see "Log properties" on page 142) for your system logs, including the event log and the audit log. Administrators can only disable/enable audit logging. All other logs are compulsory.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Log properties

Your system can generate various types of logs. When you configure logs, you can define the following:

Logs (Management Application log, Recording Server service log, Image Server service log, and Image Import service log)

Name	Description
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.
Days to log	A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Event Log

Name	Description
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.

Name	Description
Days to log	A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Audit Log

Name	Description
Enable audit logging	Audit logging is the only type of XProtect Professional logging which is not compulsory. Select/clear the check box to enable/disable audit logging.
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.
Days to log	A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file is stored for seven days. To specify another number of days (max. 9999), overwrite the value in the field. The current day's activity is always logged (provided audit logging is enabled and there is user activity). Therefore, if you specify 1, you keep one day plus the current day's activity. Note that if you specify 0 (zero), audit log files are kept indefinitely (disk space permitting).
Minimum logging interval	Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.
In sequence timespan	The number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged and reduce the size of the audit log. The default is ten seconds.

Notifications

About notifications

In case of problems with hardware, activation of motion detection on your camera or similar incidents, you can set up your system to send notifications through SMS and/or email.

Email

About email

With email notifications, you can instantly get notified when your surveillance system requires attention. Your system can automatically send e-mail notifications to one or more recipients when:

- Motion is detected
- Events occur. You can select individually for each event whether you want to receive an email notification or not.
- Archiving fails (if email notification has been selected as part of the archiving properties)

Configure email notifications

To set up email notifications, do the following:

1. Expand **Advanced Configuration**, expand **Notifications**, right-click **Email** and select **Properties**.
2. Enable the use of email by selecting the **Enable email** check box.
3. Specify required properties (see "Message Settings (email)" on page 144).
4. Choose a schedule profile to associate with your email notifications. Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.

Email (Properties)

Message Settings (email)

Specify the following message settings for email:

Name	Description
Enable	Select to enable the use of email notifications, allowing you to specify further properties.
Recipient(s)	Specify the email addresses to which the system should send email notifications. To specify more than one e-mail address, separate the e-mail addresses with semicolons (example: aa@aa.aa; bb@bb.bb; cc@cc.cc).
Subject text	Enter a subject text for email notifications.
Message text	Enter a message text for email notifications. Note that camera information as well as date and time information is automatically included in email notifications.
Variables	Click a link to include a variable to the notification. The options are: • Name of triggering event • Camera name • Trigger time (the time when the notification was registered) • Error text (for example, camera failure)
Ignore similar messages for:	Specify the number of seconds to ignore sending similar notifications. This function is to ensure that you do not receive too many notifications before you have solved the relevant problem.
Use schedule profile	Select the schedule profile you want to use. By default, you can choose between **Always On**, **Always Off** or choose **Add new...** to set up a custom schedule (see "Notification Scheduling properties" on page 149).

Attachment Settings (email)

Specify the following attachment settings:

Component	Requirement
Include images	Select the check box to include still images in email notifications. When selected, each email notification includes one or more attached still JPEG images. Attached images includes images of before the incident, after the incident and the actual incident, with the incident that triggered the notification in the middle. **Important:** If your device does not record any images while the sending of notifications are turned on, no images are included in the email notification you receive.

Component	Requirement
Number of images	The number of images you want to include in the email. You can include between 1 and 20 images.
Time between images (ms)	Minimum time (in milliseconds) to be between each image. You can set any time range between 0 and 300 seconds (5 minutes).
Embed images in email	Select the check box to embed images directly in the email.

Server Settings (email)

Specify the following server settings for email:

Component	Requirement
Sender e-mail address	Enter the email address you wish to use as the sender of the email notification.
Outgoing mail server address (SMTP)	Type the name of the SMTP (Simple Mail Transfer Protocol) server which you want to use to send the email notifications. Compared with other mail transfer methods, SMTP has the advantage that you avoid automatically triggered warnings from your email client. Such warnings may otherwise inform you that your email client is trying to automatically send email messages on your behalf. TLS (Transport Layer Security) and its predecessor, SSL (Secure Socket Layer), are supported.
Outgoing mail server port (SMTP)	Type the port for your mail server. The default port number is 25.
Server requires login	Select the check box if you must use a user name and password to use the SMTP server.
Security type	Choose the type of security you want to use.
User name	Only relevant when you have selected **Server requires login**. Specify the user name required for using the SMTP server.
Password	Only relevant if you have selected **Server requires login**. Specify the password required for using the SMTP server.
Max attachment size (MB)	Specify a maximum size of attached images.

SMS

About SMS

With SMS notifications, you can instantly get notified on your mobile device when your surveillance system requires attention. To use the SMS notification feature, you must connect a 3G/USB modem to the server on which you have installed your system.

Your system can automatically send SMS notifications when:

- Motion is detected
- Events occur. You can select individually for each event whether you want to receive an SMS notification or not.
- Archiving fails (if an SMS notification has been selected as part of the archiving properties).

Configure SMS notifications

To configure SMS notifications, do the following:

1. Expand **Advanced Configuration**, expand **Notifications**, right-click **SMS** and select **Properties**.
2. Enable the use of SMS by selecting the **Enable SMS** check box.
3. Specify required properties.
4. Choose a schedule profile to associate with your SMS notifications.

Note: Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.

SMS properties

Message Settings (SMS)

Specify the following message settings for SMS:

Component	Requirement
Enable SMS	Enables the use of SMS notifications, allowing you to specify further properties.
Recipient(s)	Indicate the telephone number of the recipient. To send SMS to more than one recipient, separate the phone numbers with a semicolon.

Component	Requirement
Message text	Specify required message text for the SMS notification. Message text must only contain the following characters: a-z, A-Z, 0-9 as well as commas (,) and full stops (.). Note that camera information, date and time information are all automatically included in SMS notifications.
Variables	Click a link to include a variable to the notification. The options are: • Name of triggering event • Camera name • Trigger time (the time when the notification was registered) • Error text (for example, camera failure)
Ignore similar messages for:	Specify the number of seconds to ignore sending similar notifications. This function is to ensure that you do not receive too many notifications before you have solved the relevant problem.
Use schedule profile	Select the schedule profile you want to use. By default, you can choose between **Always On**, **Always Off** or choose **Add new...** to set up a custom schedule (see "Notification Scheduling properties" on page 149).

Server Settings (SMS)

Specify the following server settings for SMS:

Component	Requirement
Serial port	Select the serial port to use for your USB/3G modem. The list from which you can choose ports shows open serial ports on the computer running your system.
Speed	The baud speed of your USB modem device. The default value is 9600 baud. Although you can set any custom value for the baud rate, Milestone does not recommend that you change the baud rate unless you are a highly advanced user.
SIM card PIN code	Specify PIN code for the SIM card inserted in the USB/3G modem.

Component	Requirement
SMS encoding	Different types of SMS encodings exist to accommodate various language needs in the world. XProtect Professional gives you the following options: • 7-bit • 8-bit (default) • 16-bit 7-bit encryption allows you to use up to 160 characters per SMS, however it also limits the type of characters you can use. 8-bit encryption is the standard form of encryption with more special characters allowed. It allows you to use up to 140 characters per SMS. 16-bit encryption is necessary for non-Latin alphabeat languages. Characters from, for example, Arabic, Chinese, Korean, Japanese or Cyrillic alphabet languages require 16-bit SMS encoding. If you use any of these languages in your organization, you must set your XProtect Professional to use 16-bit encoding. 16-bit has a limit of 70 characters per SMS.

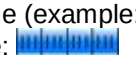
Scheduling

About scheduling of notifications

Scheduling of notifications allows you to set up schedule profiles which you can use with Email (see "Message Settings (email)" on page 144) and SMS (see "Message Settings (SMS)" on page 147) notifications.

Notification Scheduling properties

When you set up schedules to use with email or SMS notifications, specify the following:

Component	Requirement
Notification profile	Select the relevant profile (for example **Always on**) for your notification schedule profile. You specify a notification schedule profile by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

•

Central

About Central

Central Settings lets you specify the login settings required for an XProtect Central server to access the surveillance system in order to retrieve status information and alarms. If you are a user of the Milestone Integration Platform, this is also the dialog that lets you specify the login settings for the Milestone Integration Platform to access the surveillance system.

Enable XProtect Central

1. Expand **Advanced Configuration**, right-click Central and then select **Properties**.
2. Enable the use of Central connections by selecting the **Enable Milestone XProtect Central** check box.
3. Specify required properties.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Central properties

Name	Description
Enable Milestone XProtect Central connections	Enables the use of Central connections, allowing you to specify further properties.
Login Name	Type the name used for the connection between the XProtect Professional and Central servers or the Milestone Integration Platform. The name must match the name specified on the Central server or in the Milestone Integration Platform.
Password	Type the password used for the connection between XProtect Professional and Central servers or the Milestone Integration Platform. The password must match the password specified on the Central server or in the Milestone Integration Platform.
Port	Type the port number to which the XProtect Central server or the Milestone Integration Platform should connect when accessing the XProtect Professional server. The port number must match the port number specified on the XProtect Central server or in the Milestone Integration Platform. Default port is 1237.

Access control

About access control integration

The use of XProtect <Access Control Module 2014> requires that you have purchased a license that allows you to access this feature.

You can use XProtect <Access Control Module 2014> with access control systems from vendors that have a vendor-specific plug-in for XProtect <Access Control Module 2014>.

The access control integration feature introduces new functionality that makes it simple to integrate customers' access control systems with XProtect. You get:

- A common operator user interface for multiple access control systems in the XProtect Smart Client
- Faster and more powerful integration of access control systems
- More functionality (see below)

In the XProtect Smart Client, the operator gets:

- Live monitoring of access control events
- Operator aided passage for access requests
- Map integration
- Alarm definitions for access control events
- Investigation of access control events
- Centralized door state overview and control
- Cardholder information

Apart from a license, you need a vendor-specific integration plug-in installed on the event server before you can start an integration.

Wizard for access control system integration

The **Access control system integration** wizard is for step-by-step configuration of the initial integration with an access control system. Use the wizard to get through the most basic configuration tasks. You can do more detailed configuration afterwards.

Before you start the access control integration wizard make sure you have the integration plug-in installed on the event server.

Some of the fields to fill out and their default values are inherited from the integration plug-in. Therefore the appearance of the wizard may differ depending on the access control system you integrate with.

To start the wizard, select **Access Control** in the node tree, right-click, and click **Create new**.

Steps in this wizard:

Create access control system integration 152
Connecting to the access control system 152
Associated cameras 152
Final summary 152

Create access control system integration

Enter the name and specify the connection details for the access control system you want to add. The parameters that you must specify depend on the type of system, but are typically the network address of the access control system server and an access control administrator user name and password.

The video management system uses the specified user name and password to log into the access control system for retrieving the full configuration.

The integration plug-in may also define secondary parameters which are not listed in the wizard, but you can change these in **General Settings** after setting up the integration. The default values for the parameters are supplied by the plug-in or the XProtect system.

Connecting to the access control system

When the plug-in has been successfully integrated, a summary of the retrieved access control system configuration appears. Review the list to ensure that all items have been integrated before you continue to the next step of the wizard.

Associated cameras

Map access points in the access control system with the cameras in the XProtect system, to show related video for events from the doors.

You can map several cameras to one access point. The XProtect Smart Client user is then able to view video from all the cameras when investigating events, for example.

The XProtect Smart Client user is also able to add one of the cameras when configuring **Access Monitor** view items.

Licensed doors are by default enabled. Clear the check box to disable a door and thereby free a license.

Final summary

Your access control system integration has been successfully created in XProtect with default settings inherited from the integration plug-in. Client users must log into XProtect Smart Client to see and use the new access control system.

You can refine the configuration in the Management Client.

Access control properties

General Settings tab (Access Control)

Name	Description
Enable	Systems are by default enabled, meaning that they are visible in XProtect Smart Client for users with sufficient rights and that the XProtect system receives access control events. You can disable a system, for example during maintenance, to avoid creating unnecessary alarms.
Name	The name of the access control integration as it appears in the management application and in the clients. You can overwrite the existing name with a new one.
Description	Provide a description of the access control integration. This is optional.
Integration plug-in	Shows the type of access control system selected during the initial integration.
Last configuration refresh	Shows the date and time of the last time the configuration was imported from the access control system.
Refresh configuration	Click the button when you need to reflect configuration changes made in the access control system in XProtect, for example you have added or deleted a door. A summary of the configuration changes from the access control system appears. Review the list to ensure that your access control system is reflected correctly before you apply the new configuration.
Operator login required	Enable an additional login for the client users, if the access control system supports differentiated user rights. This option is only visible if the integration plug-in supports differentiated user rights.

The naming and content of the following fields are imported from the integration plug-in. Below are examples of some typical fields:

Name	Description
Address	Type the address of the server that hosts the integrated access control system.
Port	Specify the port number on the server to which the access control system is connected.

Name	Description
User name	Type the name of the user, as defined in the access control system, who should be administrator of the integrated system in XProtect.
Password	Specify the password for the user.

Associated Cameras tab (Access Control)

Provides mappings between door access points and cameras, microphones or speakers. You associate cameras as part of the integration wizard, but you can change the setup at any time. Mappings to microphones and speakers are implicit through the related microphone or speaker on the camera.

Name	Description
Doors	Lists the available door access points defined in the access control system, grouped by door. **Enabled**: Licensed doors are by default enabled. You can disable a door to free a license. **License**: Shows if a door is licensed or if the license has expired. The field is blank when the door is disabled. **Remove**: Click **Remove** to remove a camera from an access point. If you remove all cameras, the check box for associated cameras is automatically cleared.
Cameras	Lists the cameras configured in the XProtect system. Select a camera from the list, and drag and drop it at the relevant access point to associate the access point with the camera.

Access Control Events tab (Access Control)

Event categories allow you to group events. The configuration of event categories affects the behavior of access control in the XProtect system and allows you to, for example, define an alarm to trigger a single alarm on multiple event types.

Name	Description
Access Control Event	Lists the access control events imported from the access control system. The integration plug-in controls default enabling and disabling of events. You can disable or enable events any time after the integration. When an event is enabled, it is stored in the XProtect event database and is, for example, available for filtering in the XProtect Smart Client.
Source Type	Shows the access control unit that can trigger the access control event.

Name	Description
Event Category	Assign none, one or more event categories to the access control events. The system automatically maps relevant event categories to the events during integration. This enables a default setup in the XProtect system. You can change the mapping at any time. Built-in event categories are: ▸ Access denied ▸ Access granted ▸ Access request ▸ Alarm ▸ Error ▸ Warning Events and event categories defined by the integration plug-in also appear, but you can also define your own event categories, see **User-defined Categories**. **Important**: If you change the event categories in a Corporate system, ensure that the existing access control rules still work.
User-defined Categories	Allows you to create, modify or delete user-defined event categories. You can create event categories when the built-in categories do not meet your requirements, for example, in connection with defining triggering events for access control actions. The categories are global for all integration systems added to the XProtect system. They allow setting up cross-system handling, for example on alarm definitions. If you delete a user-defined event category, you receive a warning if it is used by any integration. If you delete it anyway, all configurations made with this category, for example access control actions, do not work anymore.

Access Control Actions

Actions specify the behavior of the access control system in the XProtect Smart Client, based on the configuration of the triggering events.

You can specify one or more actions related to:

- An event category
- Events from the access control system
- Events from the XProtect system

Triggering events are from a specific access control unit or from a group of access control units.

Name	Description
Trigger Event	Select from the list an event category that should trigger an action. The list includes built-in, plug-in and user-defined event categories. Select **Access control event**, to create a trigger based on specific access control events instead of an event category. Select **External event**, to create a trigger based on an input event in the XProtect system. Specify the input source in the **Source** field for each trigger.
Source	Select the source which the action affects. The options depend on the setting of the **Trigger Event** field. For event categories and access control events, select: • All doors • Individual doors • Other... Click **Other** to select multiple doors, door access points or other units in the access control system. For external event: Select the source from a list of events and input devices in the XProtect system.
Time Profile	Select the time profile in which you want the action to be performed if triggered. Configure time profiles as part of **Advanced Configuration**.
Action	Select the type of action: • Display access request notification • Go to PTZ preset • Start recording • System action For each action, specify action details. To set up multiple actions, click **Add access control action**. You can do this, for example, if you want different actions triggered by the same event depending on weekend vs. office hours.
Add access control action	Click to add and define actions as required.

Action details	Configure the parameters for an action: Display access request notification: ▸ Specify which cameras, microphones or speakers the XProtect Smart Client user connects to via the notification user interface when a given event occurs. Also specify the sound to alert the user when the notification pops up. To enable more commands in the notification, see **Add Command**. Go to PTZ preset: ▸ Specify the camera and select from the pre-configured presets a pattern for the camera and the time of return to preset when a given event occurs. Start recording: ▸ Specify the cameras that should start recording and the duration when a given event occurs. System action: ▸ Specify an action predefined in the XProtect system.
Add command	Select which commands that should be available as buttons in the access request notification dialogs in the XProtect Smart Client. Related access request commands: ▸ Enables all commands related to access request operations available on the source unit. For example **Open door**. All related commands: ▸ Enables all commands on the source unit. Access control command: ▸ Enables a selected access control command. System command: ▸ Enables a command predefined in the XProtect system. To delete a command, click **X** on the right side.

Cardholders tab (Access Control)

Use the **Cardholders** tab to review information about cardholders in the access control system.

Name	Description
Search cardholder	Type the characters of a cardholder name and it appears in the list, if it exists.

Name	Description
Name	Lists the names of the cardholders retrieved from the access control system.
Type	Lists the type of cardholder, for example: ▸ Employee ▸ Guard ▸ Guest

If your access control system supports adding/deleting pictures in the XProtect system, you can add pictures to the cardholders. This is useful if your access control system does not include pictures of the cardholders.

Name	Description
Select picture	Specify the path to a file with a picture of the cardholder. This button is not visible if the access control system manages the pictures. Allowed file-formats are .bmp, .png, and .jpg. Pictures are resized to maximize the view. Milestone recommends that you use a quadratic picture.
Delete picture	Click to delete the picture. If the access control system had a picture, then this picture is shown after deletion.

Server access

About server access

You can configure clients' access to your system's server in two ways:

- **Wizard-driven:** Specify how clients access the server and which users can use clients through guided configuration. When you use the wizard, all users that you add have access to all cameras, including new cameras added at a later stage. If this is not what you want, specify access settings, users and user rights separately.
- **Through advanced configuration:** This was known as Image Server administration in previous versions.

About registered services

Registered services displays the services installed and running on your system. It displays the following information about the individual services:

Name	Description
Enabled	Indicates if the relevant service is enabled.
Name	The name of the service.
Description	A description of the service.
Addresses	The inside and outside addresses used by the service.

You can change the inside and outside addresses for a service. To do this, click the **Edit** button and enter the relevant inside and/or outside addresses. Note that you cannot edit all services. You can delete a service registration from the system by clicking the **Delete** button. You are prompted for confirmation before the service is deleted.

Configure server access

1. Expand **Advanced Configuration,** right-click **Server Access** and select **Properties**.
2. Specify required properties for Server Access, Local IP Ranges, and Language Support and XML Encoding. Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

When you use this option, you configure client users separately from clients' access. See Add individual users, Add user groups, and Configure user and group rights.

Server access properties

Server access

When you configure server access (on page 159) (that is clients' access to the system server), specify the following:

Name	Description
Server name	Name of the XProtect Professional server as it will appear in clients. Client users with rights to configure their clients will see the name of the server when they create views in their clients.
Local port	Port number to use for communication between clients and the surveillance server. The default port number is 80; you can change the port number if port 80 is used for other purposes in your organization.

Name	Description
Enable internet access	Select the check box if the server should be accessible from the internet through a router or firewall. If you select this option, also specify the public (“outside”) IP address and port number in the following fields. When using public access, the router or firewall used must be configured so requests sent to the public IP address and port are forwarded to the local (“inside”) IP address and port of the XProtect Professional server.
Internet address	Specify a public IP address or hostname for use when the system server should be available from the Internet.
Internet port	Specify a port number for use when the system should be available from the Internet. The default port number is 80. You can change the port number if needed.
Max. number of clients	You can limit the number of clients allowed to connect at the same time. Depending on your XProtect Professional configuration and the performance of the hardware and network used, limiting the number of simultaneously connected clients may help reduce server load. If more than the allowed number of simultaneously connected clients attempt to log in, only the allowed number of clients will be allowed access. Any clients in excess of the allowed number will receive an error message when attempting to log in. By default, a maximum of ten simultaneously connected clients are allowed. To specify a different maximum number, simply overwrite the value. **Tip:** To allow an unlimited number of simultaneously connected access clients, type **0** (zero) in the **Max. number of clients** field. A four-minute session timeout period applies for client sessions on XProtect Professional. In many cases, client users may not notice this at all. However, the session timeout period will be very evident if you set the Max. number of clients value to 1. When that is the case, and the single allowed client user logs out, four minutes must pass before it will be possible to log in again.

Local IP ranges

You can specify IP address ranges which your system should recognize as coming from a local network. This can be relevant if different subnets are used across your local network.

1. Click the **Add** button.
2. In the **Start Address** column, specify the first IP address in the range.
3. In the **End Address** column, specify the last IP address in the range.

Repeat if you want to add other local IP address ranges.

Language support and XML encoding

You can select the language/character set that should be used by your system's server and clients.

Component	Requirement
Character encoding/Language	Select required language/character set. Example: If the surveillance server runs a Japanese version of Windows, select Japanese. Provided access clients also use a Japanese version of Windows, this will ensure that the correct language and character encoding is used in clients' communication with the server. If you are using a master/slave setup, remember to specify the same language/character set on all relevant servers.

Master/Slave

About master and slave

You can create a master/slave setup of your system servers. A master/slave setup allows remote users to transparently connect to more than one server at the same time. When remote users connect to the master server, they instantly get access to the slave servers as well.

You can designate one server per Software License Code (SLC) as master server and an unlimited number of slave servers. To check the connection of your slave servers, you can verify the connection to your slaves by clicking **Update Status** and let the system report the number of connected slaves back to you.

Configure master and slave servers

1. Expand **Advanced Configuration**, right-click **Master/Slave** and select **Properties**.
2. Select the **Enable as master server** check box.
3. Click **Add** to add a slave server.
4. Specify slave server properties. When ready, click **OK.**

Master/slave properties

You can set the following properties for master servers and slave servers:

Master server properties

Properties available in XProtect Enterprise and XProtect Professional only:

Name	Description
Enable as master server	Select to enable as master server.
Timeout	Set timeout of slave update. See **Update Status on Slaves** further below.
Add	Lets you add slave servers. Select **Master Server** in the list and click the **Add** button.

Properties available in XProtect Enterprise only:

Pre version 8.0 slaves	Select this to enable support of slaves running XProtect Professional versions prior to version 8.0. Selecting Pre version 8.0 slaves disables the update slave status feature for all slaves—both pre 8.0 and beyond. See **Update status on slaves** further below.

When you select **Master Server**, the **Delete** button is disabled and the **Add** button is enabled (provided you have selected **Enabled as master server**). This allows you to add slave servers to the master server, but prevents your from deleting the master server.

Slave server properties

Name	Description
Address	IP address of the slave server.
Port	Port number of the slave server.
Delete	Remove a slave server from the list of slave servers. Select the slave server in the list and click the **Delete** button.

If you want a slave server to become a master server, clear **Enable as master server** on the original master server and click **OK**. In the navigation pane, right-click the slave server which you want to become master server and select **Properties**. Then select **Enable as master server.** Next click **Add** to add slave servers to the new master server.

Update status on slaves

In the **Master Settings Summary** and **Slave Settings Summary** table area, you can verify/update added slaves by clicking **Update Status**. A status dialog runs and afterwards informs you of the status of your slave server(s).

If you select **Pre version 8.0 slaves**, it is not possible to update slave status on any slaves and **Update Status** is therefore disabled. In the **Slave Settings Summary** table, slave status on all slaves is **Not applicable**.
If you do **not** select **Pre version 8.0 slaves**, slave status for pre version 8.0 slaves is **Unreachable.** Slave status for 8.0 slaves and beyond reflects the actual status.

Users

About users

The term **users** primarily refers to users who connect to the surveillance system through their clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

You can add both types of users through the Configure User Access wizard or individually (see Add basic users (on page 163) and Add Windows users (on page 163)).

By grouping users, you can specify rights for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work. User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services. If you want to use groups, make sure you add groups before you add users: you cannot add existing users to groups.

Finally, the Administrators group is also listed under Users. This is a default Windows user group for administration purpose which automatically has access to the Management Application.

Add basic users

When you add a basic user, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that creating Windows users provides better security. If you want to include users in groups, make sure you add required groups before you add users. You cannot add existing users to groups.

You can add basic users in two ways: One is through the **Configure User Access** wizard. Alternatively, add basic users this way:

1. Expand **Advanced Configuration**, right-click **Users**, and select **Add New Basic User**.
2. Specify a user name. Specify a password, and repeat it to be sure you have specified it correctly. Click **OK**.
3. Specify General Access and Camera Access properties. These properties determine the rights of the user. Click **OK**.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add Windows users

When you add Windows users, you import users defined locally on the server (or from Active Directory®, supported in XProtect Enterprise 2013+ and XProtect Professional 2013+ only) and authenticate them based on their Windows login. This generally provides better security than the basic user concept, and it is the method Milestone recommends. If you want to include users in groups, make sure you add required groups before you add users. You cannot add existing users to groups.

Add Windows users in two ways: One is through the Manage user access wizard. Alternatively, add Windows users this way:

1. Expand **Advanced Configuration**, right-click **Users**, and select **Add New Windows User**. This opens the **Select Users or Groups** dialog.

   Note that you can only make selections from the local computer, even if you click the Locations... button.

2. In the **Enter the object names to select** box, type the relevant user name(s), then use the **Check Names** feature to verify it. If you type several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**

3. When done, click **OK**.

4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.

5. Click **OK**.

6. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Users added from a **local database** logging in with a client should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should still specify a password and any required server information.

Add user groups

User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®.

By grouping users, you can specify rights (see "Configure user and group rights" on page 165) for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work. Make sure you add groups before you add users: you cannot add existing users to groups.

1. Expand **Advanced Configuration**, right-click **Users**, and select **Add New User Group**.

2. Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

3. Click **OK**.

4. Specify General access (on page 166) and Camera access (on page 166) properties. These properties will determine the rights of the group's future members.

5. Click **OK**.

6. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

7. Now you can add users to the group: in the navigation pane, right-click the group you just created, and Add basic users **(on page 163) or** Add Windows users (on page 163) as required.

Configure user and group rights

User/group rights are configured during the process of adding users/groups, see Add basic Users (on page 163), Add Windows users (on page 163) and Add user groups (on page 164). Note that you can also add basic and Windows users through the Manage user access wizard (on page 55). However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

If you at a later stage want to edit the rights of a user or group:

1. Expand **Advanced Configuration**, expand **Users**, right-click the required user or group, and select **Properties**.
2. Edit General Access (on page 166) and Camera Access (on page 166) properties. These properties determine the rights of the user/group. Click **OK**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

User properties

User information

Name	Description
User name	Edit the user name. You can only edit this if the selected user is a Basic user. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Password	Only editable if the selected user is of the type basic user. Edit the password. Remember to repeat the password to be sure you have specified it correctly.
User type	Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

Group information

Name	Description
Group name	Edit the group name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

General access

When you add or edit basic users (see "Add basic users" on page 163), Windows users (see "Add Windows users" on page 163) or groups (see "Add user groups" on page 164), specify general access settings:

Name	Description
Live	Ability to access the **Live** tab in XProtect Smart Client.
Playback	Ability to access the **Playback** tab in XProtect Smart Client.
Setup	Ability to access setup mode in XProtect Smart Client. **Tip:** By clearing the **Live**, **Playback** and **Setup** check boxes you can effectively disable the user's/group's ability to use XProtect Smart Client. You can use this as a temporary alternative to deleting the user/group, for example while a user is on vacation.
Edit shared views	Ability to create and edit views in shared groups in XProtect Smart Client. Every user can access views placed in shared groups. If a user/group does not have this right, shared groups are protected, indicated by a padlock icon in XProtect Smart Client.
Edit private views	Ability to create and edit views in private groups in XProtect Smart Client. Views placed in private groups can only be accessed by the user who created them. If a user/group does not have this right, private groups will be protected, indicated by a padlock icon in XProtect Smart Client. Denying users the right to create their own views may make sense in some cases, for example, to limit bandwidth use. For more information about shared and private views, see the separate XProtect Smart Client documentation.
Administrator Access	Select the checkbox to allow users to access and work with the Management Application. If you have more than one Administrator member, you can clear the checkbox to ensure that other administrators cannot access the Management Application.

Camera access

When you add or edit basic users (see "Add basic users" on page 163), Windows users (see "Add Windows users" on page 163) or groups (see "Add user groups" on page 164), you can specify camera access settings.

In the list of cameras, select the camera(s) you want to work with. Note the last item in the list, **Rights for new cameras when added to the system**, with which you can allow the user/group access to any future cameras.

Tip: If the same features should be available for access for several cameras, you can select multiple cameras by pressing SHIFT or CTRL on your keyboard while you select.

For the selected camera(s), in the **Access** check box, specify if the user/group should have access to live viewing and playback at all. If so, specify if they should have access to **both** live viewing and

playback and—if this is the case—which sub-features should be available when you work with the selected camera(s). The sub-features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback.

The **Camera access settings** check boxes work like a hierarchy of rights. If the **Access** check box is cleared, everything else is cleared and disabled. If the **Access** check box is selected, but, for example, the **Live** check box is cleared, everything under the **Live** check box is cleared and disabled.

Depending on the selected column, the following default features for live or playback from the selected camera(s) give you the ability to:

Properties available in all XProtect software versions:

Live	Features
PTZ	Use navigation features for PTZ (Pan-tilt-zoom) cameras. A user/group can only use this right if the user has access to one or more PTZ cameras.
PTZ preset positions	Use navigation features for moving a PTZ camera to particular preset positions. A user/group can only use this right if the user/group has access to one or more PTZ cameras with defined preset positions.
Manage PTZ presets	Manage PTZ positions in XProtect Smart Client.
Output	Activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
Events	Use manually triggered events related to the selected camera(s). This feature is available in XProtect Smart Client only.
Incoming audio	Listen to incoming audio from microphones related to the selected camera(s). This feature is available in XProtect Smart Client only.
Manual recording	Manually start recording for a fixed time (defined (see "Manual recording" on page 79) by the surveillance system administrator).

Properties available in XProtect Enterprise and XProtect Professional only:

Outgoing audio	Talk to audiences through speakers related to the selected camera(s). This feature is available in XProtect Smart Client only.

Properties available in all XProtect software versions:

Playback	Features
AVI/JPEG export	Export evidence as movie clips in AVI format and as still images in JPEG format.
Database export	Export evidence in database format. This feature is available in XProtect Smart Client only.
Sequences	Use the **Sequences** feature when playing back video from the selected camera.
Smart search	Search for motion in one or more selected areas of images from the selected camera. This feature is available in XProtect Smart Client only.

Recorded audio	Listen to recorded audio from microphones related to the selected camera(s).

You cannot select a feature, if the selected camera does not support the relevant feature. For example, PTZ-related rights are only available if the relevant camera is a PTZ camera. Some features depend on the user's/group's General Access (on page 166) properties.

Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A, you have selected that use of the Events is allowed, for camera B, you have not allowed this. If you select both camera A and camera B in the list, the Events check box in the lower part of the window is square-filled. Another example: Camera C is a PTZ camera for which you have allowed the PTZ preset positions feature whereas camera D is not a PTZ camera. If you select both camera C and camera D in the list, the PTZ preset positions check box is square-filled.

Alarm management

When you add or edit basic users (see "Add basic users" on page 163), Windows users (see "Add Windows users" on page 163) or groups (see "Add user groups" on page 164), specify their XProtect Smart Client alarm management rights:

Name	Description
Manage	Allows users of the XProtect Smart Client to: • Manage alarms (for example, change priorities of alarms and re-delegate alarms to other users) • Acknowledge alarms—in the XProtect Smart Client's alarm list and maps. • Change state (for example from **New** to **Assigned**) of several alarms simultaneously (otherwise state must be changed on a per-alarm basis).
View	Allows users of the XProtect Smart Client to: • View alarms • Print alarms reports.
Disable	Allows users of the XProtect Smart Client to disable alarms.

Access control management

When you add or edit basic users (see "Add basic users" on page 163), Windows users (see "Add Windows users" on page 163) or groups (see "Add user groups" on page 164), specify access control settings:

Name	Description
Use Access Control	Allows the relevant user to use any access control-related features in XProtect Smart Client.

Services

About services

The following services are all automatically installed on the system server if you run a **Typical** installation. By default, services run transparently in the background on the system server. If you need to, you can start and stop services separately from the Management Application, see Start and stop services (on page 170).

Service	Description
Milestone Recording Server service	A vital part of the surveillance system. Video streams are only transferred to your system while the Recording Server service is running.
Milestone Image Server service	Provides access to the surveillance system for users who log in with XProtect Smart Client. **Note:** If the Image Server service is configured in Windows Services to log in with another account than the Local System account, for example as a domain user, installed instances of XProtect Smart Client on other computers than the surveillance server itself are not able to log in to the server using the server's host name. Instead, those users must enter the server's IP address.
Milestone Image Import service	Used for fetching pre- and post-alarm images, and storing the fetched images in camera databases. Pre- and post-alarm images is a feature available for selected cameras only that enables sending of images from immediately before and after an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with the system's pre- and post-recording feature (see "Recording" on page 91).
Milestone Log Check service	Performs integrity checks on your system's log files. For more information, see Overview of Logs.
Milestone Event Server service	Manages all alarms and map-related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.
Milestone Mobile service	Manages the communication between the Recording Server and mobile devices (such as smartphones and tablets) and between the Recording Server and web browsers.

If you run a Custom installation, you can choose not to install the Mobile server and/or the Event Server. If you do so, the Mobile service and/or the Event Server service will not be seen in your Services overview.

Start and stop services

On an system server, several services by default run in the background. If you need to, you can start and stop each service separately:

1. Expand **Advanced Configuration** and select **Services**. This displays the status of each service.
2. You can now stop each service by clicking the **Stop** button. When a service is stopped, the button changes to **Start**, allowing you to start the service again when required.

Servers

Mobile server

About Mobile server

A Mobile server handles log-ins to the system from Milestone Mobile client from a mobile device or XProtect Web Client.

Upon correct login, the Mobile server distributes video streams from relevant recording servers to Milestone Mobile client. This offers an extremely secure setup, where recording servers are never connected to the Internet. When a Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

You must install the Mobile server on any computer from which you want to access recording servers. Before you begin the installation of the Mobile server, make sure you are logged in with an account that has administrator rights. Installation cannot be successful if you use a standard user account.

About direct streaming

By default, when your system transfers video from cameras to your system, the Milestone Mobile server decodes video images from the codec used on the camera into JPEG files. This decoding process is somewhat resource-intense for the Milestone Mobile server. Direct streaming allows the Milestone Mobile server to transfer the images to XProtect Web Client in the original codec format, and, thereby, reduce the strain on the Milestone Mobile server as no decoding is necessary.

Under the Milestone Mobile server's **General** Settings, you can enable direct streaming on the Milestone Mobile server to enable the use of direct streaming for users of the XProtect Web Client. However, administrators can also select to make it mandatory for all users to use direct streaming in XProtect Web Client. If administrators enable this setting, all users will always use direct streaming. If you enable mandatory direct streaming, all instances of Milestone Mobile client will no longer be able to connect, so administrators should only use this setting if users strictly use the Milestone Mobile server to connect to XProtect Web Client.

To use direct streaming, you must install a plug-in on the PC on which you access XProtect Web Client. XProtect Web Client automatically asks users if they wish to install this plug-in (if they connect through a supported browser).

About Video push

Video push is feature in your Milestone Mobile client that allows you to use your mobile device's camera to, for example, collect evidence when you investigate an alarm or event. You do this by sending a video stream from your mobile device to your system. In the Mobile server settings, you can set up how many users should be able to use the Video push feature in the system.

About saving configuration changes in XProtect Enterprise 8.1 and streamlined software versions

The following applies to XProtect Enterprise 8.1, XProtect Professional 8.1, XProtect Express 1.1, XProtect Essential 2.1 and XProtect Go 2.1 software versions only.

If you are logged into the Milestone Mobile client and are watching one or more cameras views while at the same time changing configuration in the Management Application, the live video from the camera may freeze in the Milestone Mobile client if you click **File > Save** in the Management Application**.**

To avoid this scenario, you must restart the Milestone Mobile service manually. See the Windows Help for information about how to do this.

If you are using newer versions of XProtect, the Milestone Mobile service restarts with the other services and no user action is required.

Add/edit a Mobile server

1. Go to **Servers** > **Mobile Servers.** From the menu that appears, select **Create New**. Fill in/edit the needed properties.

IMPORTANT: If you edit settings for **Login method, All cameras view** and **Outputs and events**, while you are connected to the Milestone Mobile client, you must restart the Milestone Mobile client for the new settings to take effect.

Add a Video push channel

Each Video push channel requires a separate camera license.

To add a Video push channel (see "About Video push" on page 171), do the following:

1. On the **Video Push** tab, select the **Video push** checkbox to enable the functionality.
2. In the bottom right corner, click **Add** to add a video push channel to the **Channels** mapping.
3. Channels are mapped to devices through user names. Select a user name from a user account already set up in your system to associate with the relevant Video push channel. If you do not associate the Video push channel with an already created user, you cannot use Video push in your Milestone Mobile client when you log in.
4. Add the Video push driver as a hardware device (see "Add a Video push driver as a hardware device" on page 172) to the system. You must choose the **Manual** hardware device detection method as the Video push driver does not show up in automatic hardware searches.
5. On the **Video Push** tab, click **Find Cameras**. If successful, the newly added Video push driver appears in this list. Save your configuration to make the Video push driver ready for use.

You can remove video push channels you do not require. To do so, select the relevant channel and click **Remove** in the bottom right corner.

Add a Video push driver as a hardware device

If you add a Video push channel, you must add the Video push driver to your Management Application/Management Client. To do so:

1. Open the **Add New Hardware Wizard** in your Management Application/Management Client.
2. Choose the **Manual** option. The Video push driver will not be detected in automatic hardware searches.
3. Specify hardware device settings (see "Add hardware devices settings" on page 172) and select the hardware driver manually.
4. Once finished, your Video push driver must be associated with your Video push channel. To do so, return to your Mobile server > **Video Push** tab and click **Find Cameras**.

Add hardware devices settings

Specify the following settings when you add a Video Push driver in the **Add Hardware Devices** wizard:

Name	Description
Use:	Select if the Video push driver should added to the XProtect video management system.
Address:	Type in the Milestone Mobile server IP address.
Port:	Type in the port number for your Video push driver. The default port is 80. The port is for communication between the Milestone Mobile server and your XProtect server. **Important:** The port number you set must be identical with the port number you set when you specify your Video push settings (see "Video Push" on page 174). If the port numbers are not identical, your Video push channel will not work.
User name:	Select the same user name as associated with the Video push channel when you added (see "Add a Video push channel" on page 171) this.
Password:	Type in the password for the Video push driver. The password for your Video push driver is **Milestone** (this cannot be changed).
Hardware Driver:	Select the **Video push driver**.
Verified:	Select if the Video push driver runs on a secured HTTPS connection.

Once finished, go back to your Milestone Mobile server > **Video Push** tab and click **Find Cameras** to finish setting up the Video push channel.

Mobile server settings

General

Fill in and specify general settings for the Milestone Mobile server:

Name	Description
Server name:	Enter a name of the Milestone Mobile server.
Description:	Enter an optional description of the Milestone Mobile server.
Mobile server:	Choose between all Milestone Mobile servers currently installed to the specific XProtect system. Only Milestone Mobile servers that are running are shown in the list.
Connection type:	Choose how clients should connect to the Milestone Mobile server. You can choose between the following options: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**.
Client timeout (HTTP):	Set a time frame for how often the Milestone Mobile client must indicate to the Mobile server that it is up and running. The default value is 30 seconds. Milestone recommends that you do **not** increase the time frame.
Login method:	Select how you want to log in to the Mobile server server should take place. You can choose between the following options: **Automatic, Windows Only** or **Basic Only.**
Enable XProtect Web Client:	Enable the use of XProtect Web Client.
Enable all cameras view:	Enable/disable viewing of **All Cameras** view. This view contains all cameras on a recording server (user rights permitting).
Enable actions (events and outputs):	Enable/disable actions in Milestone Mobile clients.
Enable keyframes:	Enable/disable video stream to stream key frames only. Enabling key frames only reduces bandwidth usage.
Enable full-size images:	Enable the Milestone Mobile server to send full-size images to the MilestoneMobile client or XProtect Web Client. Note that enabling full-size images increases your bandwidth usage and that enabling this option disables all rules set up in the **Performance** settings.
Direct streaming:	Choose how to handle direct streaming in XProtect Web Client. Choose between enforcing the use of direct streaming, enforcing the use when possible or never enforcing its use.
Configuration backup:	Import or export your Milestone Mobile server configuration. Your system stores the configuration in an XML file.

Server Status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since	Shows how long the Mobile server has been running since it was last stopped.
CPU usage	Shows current CPU usage on the Mobile server.
Internal bandwidth	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column	Shows the current relation between the Mobile server and the Milestone Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: **Connected** and **Logged** In XProtect.
Bandwidth Usage column	Shows the level of bandwidth used by the Mobile server client user in question.
Live Streams column	Shows the number of live video streams currently open for the Milestone Mobile client user in question.
Playback Streams column	Shows the number of playback video streams currently open for the relevant Mobile client user.
Video Push streams	Shows the number of Video Push stream currently open for the relevant Mobile client user.
Direct Streams	Shows the number of live video streams using Direct Streaming that are currently open for the relevant Mobile user.

Video Push

If you enable Video push, specify the following settings:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your XProtect system.
Channel column	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant video push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see "Add a Video push channel" on page 171), click **Find Cameras** to search for the relevant camera.

Export

Specify the following settings for exported recordings:

Name	Description
Export	Select to enable export in clients.
Include timestamps	Select to add timestamps to exported video.
Used codec for AVI files	Choose a codec to use to encode your exported AVI video files.
Export to	Specify the location to which recordings should be exported.
Delete exported recordings older than	Enter the number of days to pass before recordings are deleted. Note that if the value is set to 1 day, exported files are deleted up to 10 minutes from the applied change, not immediately. Users can restart the Mobile server manually to make the changes take effect immediately.
Limit size of exports folder to	Enter a number to set a maximum limit for the folder to which the recordings are exported.
View exports of other users	Select this check box to enable users to be able to view exports made by other users.

Automatic exports

If you want to set up your system to automatically export video when a certain event occurs, you must set up rules to instruct the system about when to carry out automatic exports:

Enabled	Select this check box to enable automatic exports.

In the columns below the **Enabled** check box is a list of all automatically exported video. See the following details for individual automatic exports:

Name column	Name of the rule.
Item column	Item that triggers the automatic export.
Event column	Shows event that triggers the automatic export.
Camera column	Camera from which the video is recorded.
Duration column	Length of the exported video file.
Export type column	Indicates whether the export file format is database format or AVI format.

Exported recordings

In the columns, see the following details for every individual exported recording:

Name column	Name of the exported recording.

State column	State of the exported recording.
Camera column	The camera that provided the exported recording.
Timestamp column	The point of time when the export took place.
Duration column	The length of the exported recording.
User column	The name of the user who provided the exported recording.
MB column	The size of the exported recording.
Type	The type of export. This can be **Manual** or **Automatic**.

Note: Click Refresh to update the list of exported recordings shown.

Auto Export Rule window settings

When you add a new rule for automatic export to take place, specify the following:

Name	Description
Name:	Provide a name for the rule you want to create, for example **Door opened** or **Motion detected**.
Item:	Choose the item to trigger the automatic export. This can be cameras, inputs, outputs and events. If you select a camera, this will automatically be selected as the camera to record video from.
Item type:	Displays the type of selected item.
Event:	Shows event that is used to trigger the automatic export. Type of available events depends on selected item.
Camera:	Select the camera from where the video will be recorded.
Duration:	Type the amount of time the video clip should export (in seconds).
Export type:	Choose whether the exported video clip should be in the XProtect database format or if it should be exported as an AVI file.

Performance

On the **Performance** tab, you can set the following limitations on the Milestone Mobile server's performance:

Level 1

Level 1 is the default limitation placed on the Milestone Mobile server. Any limitations you set here are always applied to the Milestone Mobile's video stream.

Name	Description
Level 1	Select the check box to enable the first level of limitations to Milestone Mobile server performance.

Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 2

If you would rather like to enforce a different level of limitations that the default one in **Level 1**, you can select the **Level 2** check box instead. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or below.

Name	Description
Level 3	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Note that if you enable **Enable full-size images** on the **General** tab, none of the **Performance** levels are applied.

Log Settings

Fill in and specify the following log settings:

Name	Description
Enabled	Enable/disable logging of Milestone Mobile client's actions in a separate log file.
Log file location:	Path to where log files are saved.
Keep logs for:	Number of days to keep logs for (default 3 days).
CPU usage:	Default level of CPU usage which will trigger a warning in the log.
Internal bandwidth:	Default internal bandwidth usage which will trigger a warning in the log.
External bandwidth:	Default external bandwidth usage which will trigger a warning in the log.
Check every:	Default time frame (30 sec.) for checking warning levels.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to Mobile server. Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which you can easily access Mobile server functionality. You can:

- Open XProtect Web Client (see "Access XProtect Web Client" on page 19)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 180)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 180)
- Show/edit port numbers (on page 180)
- Edit certificate (on page 179)
- Open today's log file (see "About accessing logs and exports" on page 179)
- Open log folder (see "About accessing logs and exports" on page 179)
- Open export folder (see "About accessing logs and exports" on page 179)

- Show Mobile server status (see "About show status" on page 179)
- Access the Milestone Mobile Help website (where you find manuals, frequently asked questions (FAQs) and product demonstration videos.)

About show status

If you right-click the Mobile Server Manager and select **Show Status...** (or double-click the Mobile Server Manager icon), a window opens, showing the status of the Mobile server. You can see the following:

Name	Description
Server running since:	Time and date of the time when the Mobile server was last started.
Connected users:	Number of users currently connected to the Mobile server.
CPU usage:	How many % of the CPU is currently being used by the Mobile server.
CPU usage history:	A graph detailing the history of CPU usage by the Mobile server.

About accessing logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved.

To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall Milestone Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between your mobile device or the XProtect Web Client and the Mobile server, you must have a valid certificate for the device or web browser to accept it without warning. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install the Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you get the choice between generating a self-signed certificate or loading a file containing a certificate issued by another trusted site. If you, at a later point, want change the certificate you use, you can do this from the Mobile Server Manager.

1. Right-click the Mobile Server Manager and select **Edit Certificate...**
2. Choose whether you want to either:
   - Generate a self-signed certificate or
   - Load a certificate file.

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.
2. Wait for a few seconds while the system installs the certificate.
3. Once finished, a window opens and informs you that the certificate was installed successfully. The Mobile service is restarted for the changes to take effect.

Locate a certificate file

1. Choose the **Load a certificate file** option.
2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.
3. Fill in the password connected to the certificate file.
4. When finished, click **OK**.

Note that HTTPS is not supported on Windows XP and Windows 2003 operating systems and works on Windows Vista or newer Windows OS only.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials...**
2. Fill in the **Server URL**
3. Select what user you want to log in as:
   - Local system administrator (no credentials needed) or
   - A specified user account (credentials needed)
4. If you have chosen a specified user account, fill in **User Name** and **Password**.
5. When finished, click **OK**.

Show/edit port numbers

1. Right-click the Mobile Server Manager and select **Show/Edit Port Numbers...**
2. To edit the port numbers, fill in the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).
3. When finished, click **OK**.

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager.

To perform any of these tasks, right-click the Mobile Server Manager and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Alarms

About alarms

The Alarms feature is a Milestone Integration Platform (MIP)-based feature that uses functionality handled by the event server. It provides central overview and control of alarms in any number of system installations throughout your organization.

You can configure alarms to be generated based on either:

- **Internal events (system-related):** for example, motion, server responding/not responding, archiving problems, lack of disk space, and more.
- **External events (integrated):** for example, MIP plug-in events.

The Alarms feature also handles general alarms settings and alarm logging.

Configuring alarms

An alarm configuration may include:

- Dynamic setup of alarm handling based on users access rights
- Central overview of all components: servers, cameras, and external units
- Setup of central logging of all incoming alarms and system information
- Handling of plug-ins, allowing customized integration of other systems, for example external access control systems.

Viewing alarms

The following can play a role with regards to alarms and who can view/control/manage them and to what degree. This is because alarms are controlled by the visibility of the object causing the alarm.

- Source/device visibility: if the device causing the alarm is not set to be visible to the user, the user cannot see the alarm in the alarm list in XProtect Smart Client.
- Right to trigger manually defined events: if manually defined events are available in your system, these can determine if the user can trigger selected manually defined events in XProtect Smart Client.
- External plug-ins: if any external plug-ins are set up in your system, these may control user's rights to handle alarms.
- General access rights: can determine whether the user is allowed to (only) view or also to manage alarms.

Time profiles for alarms

Alarms can be based on time profiles (for alarms) (see "Add a time profile (for alarms)" on page 183). Time profiles for Alarms are periods of time to use when you create alarm definitions. You can, for example, create a time profile for alarms covering the period from 2.30 PM till 3.30 PM on Mondays

and use that time profile to make sure that certain alarm definitions are only enabled within this period of time.

Alarms and XProtect Central

To a large extent, the Alarms feature covers the same functionality as XProtect Central.

However, configuration of former XProtect Central functionality is now included in the Alarms feature.

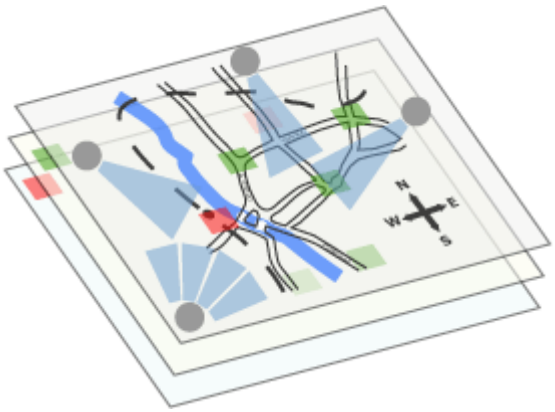
XProtect Central was an independent product consisting of two parts: a dedicated server and a number of dedicated clients. Alarms, on the other hand, is an integrated part of your system. This means that much configuration needed in XProtect Central has become redundant with the introduction of Alarms. Client-wise, the Alarms feature uses XProtect Smart Client. However, you must still configure the features Alarms, Time Profiles (for Alarms) and General Settings in the Management Application. These features are very similar to XProtect Central. You cannot reuse old alarm and map definitions from XProtect Central. You must redefine your alarms and maps definitions in the Alarms feature.

Alarms appear in the alarm list in XProtect Smart Client. Here, you can view and manage alarms to ease overview and to delegate and handle alarms. You can, for example reassign alarm, change their status or comment on alarms.

You can integrate alarms with the map functionality (see "About maps" on page 182). The Alarms feature is a powerful monitoring tool, providing instant overview of alarms and possible technical problems.

About maps

With maps as an integrated part of alarms, you get a physical overview of your surveillance system: with the possibility to assign cameras to a map, you can always tell where alarms originate, which cameras are placed where, and in what direction are they pointing. Also, you can use maps to navigate from large perspectives to detailed perspectives, and vice versa: for example, a state map can have hot zones (small icons on the map) that point to more detailed maps of cities, neighborhoods, streets, floor plans, and so on.



Example: Hierarchy of maps

All user-interaction with maps, including adding and maintaining maps, takes place in XProtect Smart Client. For detailed information, see the XProtect Smart Client documentation.

Example: Map in XProtect Smart Client

In order to use maps, the Event Server service must be running. The Event Server service is automatically included if you run a **Typical** installation of your surveillance server installation (see "Install your system software" on page 27).

Add an alarm

For a detailed overview of Alarms and how the feature works, see About alarms (on page 181).

To add/configure an alarm, do the following:

1. Expand **Alarms**, right-click **Alarm Definition** and select **Create New**.
2. Specify required properties (see "Alarms definition" on page 184). Click **OK**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a time profile (for alarms)

Time profiles are periods of time used for the Alarms feature only.

To add a time profile for an alarm, do the following:

1. Expand **Alarms**, right-click **Time Profiles**, and select **Create New**. The small month overview in the top right corner of the **Time Profile Properties** window can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.
2. In the calendar, select the **Day View, Week View, or Month View** tab, then right-click inside the calendar and select either **Add Single Time...** or **Add Recurring Time...**.
3. If you select **Add Single Time...**, specify **Start time** and **End time**. If the time is to cover whole days, select the **All-day event** box.
   —or—
   If you select **Add Recurring Time...**, specify time range, recurrence pattern, and range of recurrence. Click **OK**.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring.

Analytics events are typically data received from external third-party video content analysis (VCA) providers. An example of a VCA-based system could be an access control system.

Alarms properties

Alarms definition

When you configure Alarm definitions (see "Add an alarm" on page 183), specify the following:

Name	Description
Enable	Enables the Alarms feature.
Name	Enter a name. The alarm's name appears whenever the alarm is listed. Alarm names do not have to be unique.
Description	Enter a description (optional).
Triggering event	This first list shows both system-related events and events from plug-ins (for example access control systems or similar). From the second list, select the event message to use when the alarm is triggered.
Sources	Select which cameras and/or other devices the event should originate from in order to trigger the alarm. Plug-in defined sources, for example license plate recognition, access control systems and MIP-plugins appear in the list if installed. Your options depend upon which type of event you have selected.
Time profile	If you select **Time profile**, you must select when the alarm should be enabled for triggering. If you have not defined alarm time profiles (see "Add a time profile (for alarms)" on page 183), you will only be able to select **Always**. If you have defined one or more time profiles, they will be selectable from this list.
Event based	If you select **Event based,** you must select which events should start and stop the alarm. Events available for selection are hardware events defined on cameras, video servers and input. You can also use global/manual event definitions (see "Add a manual event" on page 112). Note that when you select **Event based**, you cannot define alarms based on outputs—only on inputs.
Time Limit	Select the time-limit within which the operator must respond to the alarm.
Events triggered	Select the event to be triggered if the operator does not react withing the time limit specified in **Time limit**. This could be, for example, sending an email, SMS or similar.

Name	Description
Related cameras	Select (a maximum of 15) cameras for inclusion in the alarm definition even though they are not themselves triggering the alarm. This can be relevant, for example, if you have selected an external event message (such as a door being opened) as the source of your alarm. By defining one or more cameras near the door, you could attach the cameras' recordings of the incident to the alarm.
Related map	Select a map to associate with the alarm definition. The selected map is automatically be shown in XProtect Smart Client whenever the alarm is listed. This might help you to quicker identify the physical location of the alarm.
Initial alarm owner	Select a default user responsible for the alarm. You can only select from users allowed to view **all** cameras and/or other devices selected as source(s) for the event causing the alarm.
Initial alarm priority	Select a priority (**High**, **Medium** or **Low)** for the alarm. Priorities can be used for sorting purposes and workflow control in the Smart Client.
Initial alarm category	Select a category to which the alarm should initially be assigned. This could be, for example, **Building01**, **Burglary**, **ElevatorEast** or similar, depending on which categories have been defined.
Event triggered by alarm	Define an event to be triggered by the alarm in the Smart Client (if needed).
Auto-close alarm	Select if the alarm should automatically be closed upon a particular event. This is possible for alarms triggered by some (but not all) events.

See also Alarm data settings (on page 185) and Alarm sound settings (see "Sound settings" on page 186) for further information on how to configure alarm settings.

Alarm data settings

When you configure alarm data settings, specify the following:

Alarm Data Levels **tab,** Priorities

Name	Description
Level	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers **1**, **2** or **3)**. These priority levels are used to configure the **Initial alarm priority** setting (see "Alarms definition" on page 184).
Name	Type a name for the entity. You can create as many as you like.
Sound	Select the sound to be associated with the alarm. Use one if the default sounds or add more in Sound Settings (on page 186).

Alarm Data Levels tab, States

Level	In addition to the default state levels (numbers **1**, **4**, **9** and **11,** which can not be edited or reused), add new states with level numbers of your choosing. These state levels are only visible in the Smart Client's **Alarm List**.
Name	Type a name for the entity. You can create as many as you like.

Alarm Data Levels tab, Categories

Level	Add new categories with level numbers of your choosing. These category levels are used to configure the **Initial alarm category** setting (see "Alarms definition" on page 184).
Name	Type a name for the entity. You can create as many as you like.

Alarm List Configuration tab

In **Available columns,** use **>** to select which columns should be available in the XProtect Smart Client **Alarm List**. Use **<** to clear selection. When done, **Selected columns** should contain the items to be included.

Reasons for Closing tab**Enable**	Select to enable that all alarms must be assigned a reason for closing before they can be closed.
Reason	Add reasons for closing that the user can choose between when closing alarms. Examples could be "**Solved-Trespasser**" or "**False Alarm**". You can create as many as you like.

Sound settings

When you configure Sound Settings, specify the following:

Name	Description
Sounds	Select the sound to be associated with the alarm. The list of sounds contain a number of default Windows sounds. These cannot be edited. However, you can add new sounds of the file type .wav, but only if these are encoded in Pulse Code Modulation (PCM). Although the default sounds are standard Windows sound-files, local Windows settings might cause these to sound different on different machines. Some users might also have deleted one or more of these sound-files and will therefore be unable to play them. To ensure an identical sound all over, you should import and use your own .wav files encoded in PCM.
Add	Lets you add sounds. Browse to the sound to upload one or several .wav files.
Remove	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.

Name	Description
Test	Lets you test the sound. In the list, select the sound. The sound will be played once.

Time profile

When you configure Time profiles (see "Add a time profile (for alarms)" on page 183), specify the following:

Component	Requirement
Name	Type a name for the time profile.
Description	Enter a description (optional).
Add Single Time	Right-click the calendar and select **Add Single Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**.
Add Recurring Time	Right-click the calendar and select **Add Recurring Time**. Specify the time range, recurrence pattern, and range of recurrence.
Edit Time	Right-click the calendar and select **Edit Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**. When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring. If you want your time profile to contain additional periods of time, add more single times or recurring times.

MIP plug-ins

About MIP plug-ins

If you install MIP (Milestone Integration Partner) plug-ins to your system, find the plug-ins in the navigation pane. Expand **Advanced Configuration** > **MIP Plug-ins**.

You can assign MIP-related user rights to users and user groups. Expand **Advanced Configuration**, expand **Users**, right-click the relevant user and select **Properties**. Under the **Alarm Management** tab, a tab that allows access to MIP settings for the selected user is located.

Settings

About automatic device discovery

Automatic device discovery allows you to automatically add hardware devices to your system as soon as you connect these to your network. When you enable automatic device discovery, your system configures and set ups cameras automatically without the need for any user interaction, making the camera instantly accessible in XProtect Smart Client's default view after the automatic installation has completed.

Note that:

- Not all cameras support automatic device discovery.
- Cameras respond differently to automatic device discovery. The systems adds some devices (such as Axis models P3301 and P3304) to the system automatically, while some devices from other vendors (such as Sony models SNC-EB520, EM520 and E521) you must turn off and back on again before they are automatically added to your system.
- You must still manually activate licenses for your camera. This is to ensure that you only activate cameras set up in an environment with multiple servers on one of the servers.

Disable information collection

1. In the Management Application toolbar, click **Options** > **Settings** > **Privacy Options**.
2. On the **Privacy Options** tab, clear the **Yes, I would like to improve XProtect Professional** check box.
3. Click **OK**.

Change default file paths

To change any of the default file paths:

1. If you want to change the configuration path, stop all services. This step is not necessary if you want to change the default recording or archiving path.
2. On the Management Application menu bar, select **Options** > **Default File Paths...**
3. You can now overwrite the necessary paths. Alternatively, click the browse button next to the field and browse to the location. For the default recording path, you can only specify a path to a folder on a **local** drive. If you are using a network drive, you cannot save recordings if the network drive becomes unavailable.

   If you change the default recording or archiving paths and there are existing recordings at the old locations, you must select whether you want to move the recordings to the new locations (recommended), leave them at the old locations, or delete them.

4. Once changes are confirmed, restart all services.

Options

General

In the General settings, you can change a number of settings that affect the general behavior and look of the Management Application.

Automatic device discovery

Automatic device discovery (see "About automatic device discovery" on page 188) is turned off by default in your system. Select the check box to enable this functionality. If the camera should use an additional user name and password besides the camera's default user name and password, select the **Use the camera's default user name and password as well as the following credentials** check box and type the relevant credentials.

Note: Not all devices support automatic device discovery. If your system does not detect your camera and add it to your system, you must manually add the camera.

Customer Dashboard

Choose if your system should send system information to the Customer Dashboard.

System mode

Important: Do **not** change system mode unless you are absolutely sure that you want the new setting to be in effect immediately after saving.

At some point in time when you save recordings on your system, the storage you save recordings on may become full. Your system offers you two system modes which handle this scenario differently, **Classic mode** and **Evidence collection mode**.

- **Classic mode** means that the system automatically deletes the oldest saved recordings in order to make room for new recordings. This is how saved recordings have been handled so far in all previous versions of your system. When you remove a hardware device in the Management Application, recordings from the relevant device are deleted from your storage. You can no longer play back recordings from the removed camera in XProtect Smart Client as these recordings will be deleted from your storage.

- **Evidence collection mode** means that the system stops recording when you reach full storage capacity. All your old recordings are kept in the storage and the system does not save any new recordings. This ensures that video recorded as evidence is never deleted automatically and remains on the hard disk drive until you change system settings in your system or you manually remove the recordings from your storage. Similarly, if you remove a hardware device from the Management Application, recordings from the device are still kept on your storage. You can playback recordings in XProtect Smart Client even if you have removed the device in the Management Application.

Summary:

	Classic mode	Evidence collection mode
When the storage on which you are recording becomes full	The system deletes oldest recordings to make room for new recordings.	The system stops saving new recordings and keeps the oldest recordings.
When you delete a device in the Management Application	The system deletes all recordings from the removed device.	The system keeps all recordings from the removed device.
Playback in XProtect Smart Client	If you have removed the device from the Management Application, playback is no longer possible in XProtect Smart Client because the system deletes recordings from the device when you remove it.	Even if you have removed the device from the Management Application, playback is still possible in XProtect Smart Client as the system keeps the recordings.
Retention time	You can set and customize retention time for your recordings.	You cannot set retention time for your recordings as your system never deletes recordings.

Choose a system mode that fits your system needs. Most users need the most recent recordings to be available in their storage and should select **Classic** mode. **Evidence** mode provides an alternative in cases where all recorded video is considered evidence and therefore must remain on your storage.

Important: Evidence Collection mode is only supported in XProtect Enterprise 2013+. If you run your system in trial mode, only **Classic** mode is available.

Important: If you have upgraded from a previous version of your system, for example XProtect Enterprise 8.1, **Classic** mode is the default selection in your system. You must manually change your selection to use **Evidence** mode.

Language

The Management Application is available in several languages. From the list of languages, select the language you want to use. Restart the Management Application to make the change of language take effect.

User Interface

You can change the way the Management Application behaves. For example, by default, the Management Application asks you to confirm many of your actions. If you feel this is not necessary, you can change the behavior of the Management Application to not ask you again. Go to **User Interface** to make changes for each action.

Examples of actions you can change:

- When you attempt to delete a hardware device, should the Management Application ask you to confirm that you want to delete the hardware device, or should it delete the hardware device straight away without asking?
- Depending on the system you are using, you may have a limit on the number of cameras you can use in your system. Select if the system should warn you if you add more cameras than the allowed number of cameras.

- If your system should show live video when you preview camera or if you would rather see a snapshot or no preview of the camera.

Click **Restore Default Settings** below the behavior list to restore your system to its default behavior.

Default File Paths

Your system uses a number of default file paths:

File paths	Description
Default recording path for new cameras	All new cameras you add use this path by default for storing recordings. If required, you can change individual cameras' recording paths as part of their individual configuration (see "Recording and archiving paths" on page 92), but you can also change the default recording path so all new cameras you add use a path of your choice.
Default archiving path for new cameras	All new cameras you add use this path by default for archiving (see "About archiving" on page 126). If required, you can change individual cameras' archiving paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add use a path of your choice. Note that camera-specific archiving paths are not relevant if you use dynamic path selection (see "Dynamic path selection (properties)" on page 73) for archiving.
Configuration path	The path by default used for storing your system configuration.

Analytics Event Settings

Analytics Event Settings let you specify the following:

Name	Description
Enabled	Lets you enable the analytics event feature
Port	Specify the port used by this service. Default port is 9090. Make sure that relevant VCA tool providers also use this port number. If you change the port number, make sure that VCA tool providers change their port number accordingly.

All network addresses or Specified network addresses	Specify whether events from all IP addresses/host names are accepted, or only events from IP addresses/host names specified in a list—see the following. In the **Address** list specify a list of trusted IP addresses/host names that you want this service to recognize. The list is used to filter incoming data so that only events from certain IP addresses/host names are allowed. Both Domain Name System (DNS) and IPv4 address formats can be used in the list. You have two ways of adding addresses to the list: either manually or by importing an external list of addresses. Manual entering: type the required IP address/host name in the address list. Repeat for each required address.
Import	Click the **Import...** button to browse for the required external list of addresses. To import an external list, the list must be saved in a .txt file format and each IP address or host name must appear on a separate line in the file. Windows' simple text editor Microsoft Notepad is an excellent tool for creating such .txt files.

Event Server Settings

Specify the following Event Server settings:

Name	Description
Keep closed alarms for	Specify the number of days for which to keep closed alarms, that is alarms in the states **Closed**, **Ignore**, and **Reject**. This is normally set to a low number, such as three days, but you can define any number up to 99999 days, server space permitting. You can use the value 0 to indicate keep closed alarms indefinitely (server space permitting).
Keep all other alarms for	Specify the number of days for which to keep all other alarms, meaning alarms not in the states **Closed**, **Ignore**, and **Reject**. This is normally set to a somewhat higher number, such as 30 days, but you can define any number up to 99999 days, server space permitting. You can use the value 0 to indicate that you want to keep all other alarms indefinitely, server space permitting. IMPORTANT: Alarms often have associated video recordings. While the alarm information itself is stored on the event server, the associated video recordings are fetched from the relevant surveillance system server when users wish to view them. Therefore, if it is vital that you have access to video recordings from all your alarms, make sure that video recordings from relevant cameras are stored on relevant surveillance system servers for at least as long as you intend to keep alarms on the event server.
Keep logs for	Specify the number of days for which to keep the Alarms log. Default is 30 days. The value of 0 indicates that you want to keep logs indefinitely (server space permitting).

Name	Description
Log server communication	Specify if you want to save a separate log of server communication in addition to the regular log for the number of days specified.

System maintenance

Back up and restore configuration

About back up and restore of configuration

Milestone recommends that you make regular backups of your system configuration (cameras, schedules, views, and so on) as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

Back up system configuration

The following describes how to back up your configuration in XProtect Professional 7.0. If you need information about how to back up a configuration from an earlier version of the system, see Upgrade from a previous version (see "Upgrading from one product version to another product version" on page 30).

In the following, we assume that you have not changed your system's default configuration path (see "Default File Paths" on page 191), which is **C:\Program Data\Milestone\Milestone Surveillance** on servers running all supported operating systems. If you have changed the default configuration path, you must take your changes into consideration when using the method described in the following.

The backup described here is a backup of your entire surveillance system setup (including, among other things, log files, event and Matrix configuration, restore points, view groups as well as Management Application and XProtect Smart Client configuration). Alternatively, you can export your configuration as a backup (see "Export and import management application configuration" on page 198), which is limited to the Management Application configuration.

To back up:

1. Make a copy of the folder **C:\Program Data\Milestone\Milestone Surveillance** and all of its content.
2. Open the folder **C:\Program Files\Milestone\Milestone Surveillance\devices**, and verify if the file **devices.ini** exists. If the file exists, make a copy of it. The file exists if you have configured video properties for certain types of cameras. For such cameras, changes to the properties are stored in the file rather than on the camera itself.
3. Store the copies away from the server, so that they are not affected if the server is damaged, stolen or otherwise affected.

Remember that a backup is a snapshot of your system configuration at the time of backing up. If you later change your configuration, your backup does not reflect the most recent changes. Therefore, back up your system configuration regularly. When you back up your configuration as described, the backup includes restore points. This allows you to not only restore the backed-up configuration, but also to revert to an earlier point in that configuration if you need to.

Restore system configuration

1. If you use the system on a server running any supported operating system, copy the content of the backed-up **Milestone Surveillance** folder into **C:\Program Data\Milestone\Milestone Surveillance.**
2. If you backed up the file **devices.ini**, copy the file into **C:\Program Files\Milestone\Milestone Surveillance\devices.**

Back up and restore alarm and map configuration

It is important that you regularly back up your alarm and map configurations. You do this by backing up the event server, which handles your alarm and map configuration as well as the Microsoft® SQL Server Express database, which stores your alarm data. This enables you to restore your alarm and map configuration in a possible disaster recovery scenario. Backing up also has the added benefit that it flushes the SQL Server Express database's transaction log.

When you back up and restore alarm and/or map configuration, you must do it in the following order:

Prerequisites

- **You must have administrator rights on the SQL Server Express database** when you back up or restore your alarm configuration database on the SQL Server Express. Once you are done backing up or restoring, you only need to be a database owner of the SQL Server Express database.
- **Microsoft® SQL Server Management Studio Express**, a tool you can download for free from www.microsoft.com/downloads. Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your existing surveillance system server and on a possible future surveillance system server (you will need it for backup as well as restoration).

Step 1: Stop the Event Server service

Stop the event server service to prevent configuration changes from being made:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click the Event Server, click **Stop**.

This is important since any changes made to alarm configurations—between the time you create a backup and the time you restore it—will be lost. If you make changes after the backup, you must make a new backup. Note that the system does not generate alarms while the Event Server service is stopped. It is important that you remember to start the service again once you have finished backing up the SQL database.

Step 2: Back up alarms data in SQL Server Express database

If you do not have **SQL Server Management Studio Express**, you can download it for free from www.microsoft.com/downloads.

1. Open Microsoft SQL Server Management Studio Express from Windows' **Start** menu by selecting **All Programs** > **Microsoft SQL Server 2008 > SQL Server Management Studio Express**.
2. When you open the tool, you are prompted to connect to a server. Specify the name of the required SQL Server and connect with administrator user credentials. You do not have to type the name of the SQL server: if you click inside the Server name field and select **<Browse for more...>**, you can select the SQL Server from a list instead.
3. Once connected, you see a tree structure in the **Object Explorer** in the left part of the window. Expand the SQL Server item, then the **Databases** item, which contains your entire alarm configuration.
4. Right-click the **VIDEOOSDB** database, and select **Tasks** > **Back Up...**
5. On the **Back Up Database** dialog's **General** page, do the following:
   - Under **Source**: Verify that the selected database is **VIDEOOSDB** and that the backup type is **Full**.
   - Under **Destination**: A destination path for the backup is automatically suggested. Verify that the path is satisfactory. If not, remove the suggested path, and add another path of your choice.
6. On the **Back Up Database** dialog's **Options** page, under **Reliability**, select **Verify backup when finished** and **Perform checksum** before writing to media.
7. Click **OK** to begin the backup. When backup is finished, you will see a confirmation.
8. Exit Microsoft SQL Server Management Studio Express.

Step 3: Reinstall your system

Do not install your surveillance software on a mounted drive. A mounted drive is a drive that is attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter. If you use mounted drives, critical system features may not work as intended. You do not, for example, receive any warnings if the system runs out of disk space.

Before you start: Shut down any existing surveillance software.

1. Run the installation file. Depending on your security settings, you may receive one or more security warnings. Click the **Run** button if you receive a warning.
2. When the installation wizard starts, select language for the installer and then click **Continue**.
3. Select if you want to install a trial version of your system or indicate the location of your license file.
4. Read and accept the license agreement, and indicate if you want to participate in the Milestone data collection program.
5. Select **Typical** or **Custom** installation. If you select **Custom** installation, you can select application language, which features to install and where to install them.
6. Let the installation wizard complete.

You can now begin to configure your system through its Management Application. For more information, see Get your system up and running (on page 33).

Step 4: Restore alarms data in SQL Server Express database

Luckily, most users never need to restore their backed-up alarm data, but if you ever need to, do the following:

1. In the Windows Start menu, open Microsoft SQL Server Management Studio Express.
2. Connect to a server. Specify the name of the required SQL Server, and connect using the user account the database was created with.
3. In the **Object Explorer** on the left, expand **SQL Server** < **Databases**, right-click the **VIDEOOSDB** database, and then select **Tasks** > **Restore** > Database...
4. In the **Restore Database** dialog, on the **General** page, under **Source for restore,** select **From device** and click <Browse for more...>, to the right of the field. In the Specify Backup dialog, make sure that **File** is selected in the **Backup media** list**.** Click **Add.**
5. In the **Locate Backup File** dialog, locate and select your backup file **VIDEOOSDB.bak**. Then click **OK.** The path to your backup file is now listed in the **Specify Backup** dialog.
6. Back on the **Restore Database** dialog's **General** page, your backup is now listed under **Select the backup sets to restore**. Make sure you select the backup by selecting the check box in the **Restore** column.
7. Now go to the **Restore Database** dialog's **Options** page, and select **Overwrite the existing database**. Leave the other options as they are, and then click **OK** to begin the restoration. When the restore is finished, you see a confirmation.
8. Exit Microsoft SQL Server Management Studio Express.

Note: If you get an error message telling you that the database is in use, try exiting Microsoft SQL Server Management Studio Express completely, then repeat steps 1-8.

Step 5: Restart the Event Server service

During the restore process, the Event Server service is stopped to prevent configuration changes being made until you are done. Remember to start the service again:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click the Event Server, click **Start**.

About the SQL Server Express transaction log and reasons for flushing it

Each time a change in the system's alarm data take place, the SQL Server logs the change in its transaction log. The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server Express database. The SQL Server by default stores its transaction log indefinitely, and, therefore, the transaction log builds up more and more entries over time.

The SQL Server's transaction log is by default located on the system drive, and if the transaction log just keeps growing, it may in the end prevent Windows from running properly. Flushing the SQL

Server's transaction log from time to time is therefore a good idea, however flushing it does not in itself make the transaction log file smaller, rather it prevents it from growing out of control. Your system does not, however, automatically flush the SQL Server's transaction log at specific intervals. This is because users have different needs. Some want to be able to undo changes for a very long time, others do not care.

You can do several things on the SQL Server itself to keep the size of the transaction log down, including truncating and/or shrinking the transaction log (for numerous articles on this topic, go to support.microsoft.com (see http://support.microsoft.com) and search for SQL Server transaction log). However, backing up the system's database is generally a better option since it flushes the SQL Server's transaction log and gives you the security of being able to restore your system's alarm data in case something unexpected happens.

Export and import management application configuration

You can export the current configuration of your Management Application, either as a safety measure in order to have a backup file of your configuration, or as a clone allowing you to use a similar Management Application configuration elsewhere. You can, at a later time, import previously exported Management Application configurations.

Export Management Application configuration as backup

With this option, all relevant Management Application configuration files are combined into one single .xml file, which you can specify a location for. Note that if there are unsaved changes to your configuration, these are automatically saved when you export the configuration.

1. In the Management Application's **File** menu, select **Export Configuration - Backup**.
2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click **Save**.

If you intend to set up an identical version of your surveillance system elsewhere, **do not** export your configuration as **backup**, since this may lead to the same device information being used twice, in which case clients may get the following error message: **Application is not able to start because two (or more) cameras are using the same name or ID.** Instead, export your configuration as a **clone**. When you export as a clone, the export takes into account the fact that you are not using the exact same physical cameras, etc. even though your new system may otherwise be identical to your existing one.

Note that there is a difference between this Management Application configuration backup and the system configuration backup done from the Milestone Surveillance folder because these are two different things. The backup described here is limited to a backup of the Management Application configuration. The type of system configuration backup done from the Milestone Surveillance folder is a backup of your entire surveillance system setup (including, among other things, log files, event configuration, restore points, view groups as well as the Management Application and XProtect Smart Client configuration).

Export Management Application configuration as clone

With this option, all relevant Management Application configuration files are collected, and GUIDs (Globally Unique IDentifiers, unique 128-bit numbers used for identifying individual system components, such as cameras) are marked for later replacement. GUIDs are marked for later replacement because they refer to specific components (cameras and so on). Even though you wish to use the cloned configuration for setting up a new similar system using similar types of cameras, the

new system does not use the exact same physical cameras as the cloned system. When you use the cloned configuration later in a new system, the GUIDs are replaced with GUIDs representing the specific components of the new system.

After you have marked GUIDs for replacement, the configuration files are combined into one single .xml file, which you can then save at a location specified by you. Note that if there are unsaved changes to your configuration, they are automatically saved when you export the configuration.

1. In the Management Application's **File** menu, select **Export Configuration - Clone**.
2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click **Save**.

Import previously exported Management Application configuration

The same import method is used regardless of whether the Management Application configuration was exported as a backup or a clone.

1. In the Management Application's **File** menu, select **Import Configuration**.
2. Browse to the location from which you want to import the configuration, select the relevant configuration file, and click **Open**.
3. Only relevant if the system into which you import the configuration contains devices (cameras, etc.) which are not present in the imported configuration: you are asked whether you want to delete or keep recordings from affected devices. If you want to keep the recordings, note that they are not accessible until you add the affected devices to the system again. Select the option you need, and click **OK**.
4. Expand **Advanced Configuration,** and select **Services**.
5. For the Recording Server and Image Server services respectively, click the **Restart** button. Restarting the two services applies the imported Management Application configuration.

Import changes to configuration

You can import changes to a configuration. This can be relevant if you install many similar systems, for example in a chain of shops where the same types of server, hardware devices, and cameras are used in each shop. In such cases, you can use an existing configuration as a template for the other installations. However, since the shops' installations are not exactly the same (the hardware devices and cameras are of the same type, but they are not physically the same, and therefore they have different MAC addresses), there needs to be an easy way of importing changes to the template configuration.

This is why you can import changes about hardware devices and cameras as comma-separated values (CSV) from a file:

1. From the menu bar, select **File** > **Import Changes to Configuration...**
2. Select **Online verification** if the new hardware devices and cameras listed in your CSV file are connected to the server and you want to verify that they can be reached.
3. Point to the CSV file, and click the **Import Configuration from File** button.

Restore system configuration from a restore point

Restore points allow you to return to a previous configuration state. Each time you apply a configuration change in the Management Application, a new restore point is created.

All restore points in the current and previous five sessions are stored and can be selected again. A new session begins each time you start the Management Application as well as each time you save the whole configuration, for example by clicking the **Save Configuration** button in the Management Application's toolbar. For sessions older than the last five sessions, only the latest restore point of each session is stored. With the **Number of old sessions to keep** field, you can control how many old sessions are kept.

When you select to restore a configuration from a restore point, the configuration from the selected restore point is applied and used once the services are restarted.

If you have added new cameras or other devices to the system after the restore point was created, they are missing if you load the restore point. This is because they were not in the system when the restore point was created. In such cases, you are notified and must decide what to do with recordings from the affected devices.

1. From the **File** menu, select **Load Configuration from Restore Point...**
2. In the left part of the **Restore Points** dialog, select the relevant restore point.
3. Click the **Load Restore Point** button.
4. If you are sure that you want to overwrite the current configuration with the one from the selected restore point, click **OK**.
5. Only relevant if the current configuration contains cameras or other devices which were not present in the selected restore point: you are asked whether you want to delete or keep recordings from affected devices. If you keep the recordings, note that you cannot access them until you add the affected devices to your system again. Select the relevant option, and click **OK**.
6. Click **OK** in the Restore Points dialog.
7. Expand **Advanced Configuration**, and select **Services**.
8. For the Recording Server and Image Server services respectively, click the **Restart** button. When the two services are restarted, the configuration from the selected restore point is applied.

Note: When you select a restore point, you can see information about the configuration state at the selected point in time in the right part of the dialog. This can help you select the best possible restore point.

Glossary of Terms

Symbols & Numeric

360 degrees panomorph support

Cameras with 360 degrees panomorph support offer—as the name indicates—360 degree coverage and can survey an entire area without blind spots or distorted images.

A

Administrator

1) System administrator. 2) In previous versions of your system: the main application used by system administrators for configuring the surveillance system server. Now called the Management Application.

Analytics Events

Analytics events are data received from an external third-party video content analysis (VCA) provider. An example of a VCA-based system is an access control system. Analytics events integrates seamlessly with the **Alarms** feature.

API

Application Program Interface—set of tools and building blocks for creating or customizing software applications.

Aspect ratio

The height/width relationship of an image.

ATM

Automatic teller machine—machine that dispenses money when a personal coded card is used.

AVI

A popular file format for video. Files in this format carry the .avi file extension.

C

Carousel

A feature for displaying video from several cameras, one after the other, in a single camera position. The required cameras and the intervals between changes are specified by the XProtect Professional administrator. The carousel feature is available, if configured, in the Smart Client.

Central

XProtect Central is a feature that provides a complete overview of status and alarms from any number of the system's servers, regardless of location.

Codec

A technology for compressing and decompressing audio and video data, for example, in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

CSV

Comma-separated values data format that stores tabular data, where the lines represent rows in a table and commas define the columns, in a simple file. For example, data about cameras may appear as comma-separated values in a .csv file, which you can then import into your system. It is an effective method if you set up several similar systems.

D

Device

In XProtect Professional : a camera, video encoder, input device, or output device connected to a recording server.

DirectX

A Windows extension providing advanced multimedia capabilities.

DNS

Domain Name System—system allowing translation between alphabetic host names (for example, mycomputer) or domain names (for example, www.mydomain.com) and numeric IP addresses (for example, 192.168.212.2). Many people find alphabetic names easier to remember than numeric IP addresses.

Driver

A program used for controlling/communicating with a device.

DST

Daylight saving time: temporarily advancing of clocks during the summer so that afternoons have more daylight and mornings have less.

Dual stream

Some cameras support two independent streams (which can be sent to the recording server): one for live viewing and another for playback purposes. Each stream has its own resolution, encoding, and frame rate.

DVR

Digital video recorder—device that records video in a digital format to a hard disk drive embedded in the DVR itself.

E

Event Server

A server that stores and handles incoming alarm data and events from all XProtect Professional servers. The Event Server enables powerful monitoring and provides an instant overview of alarms and possible technical problems within your systems.

F

Fisheye

A type of lens that allows the creation and viewing of 360-degree images.

FPS

Frames per second—measurement indicating the amount of information contained in a motion video. Each frame represents a still image, but when frames are displayed in succession, the illusion of motion is created. The higher the FPS, the smoother the motion appears. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame rate

A measurement indicating the amount of information contained in motion video—typically measured in FPS.

G

Generic events

XProtect Professional can receive and analyze input in the form of TCP or UDP data packages which, if they match specified criteria, can be used to generate events. Such events are called generic events.

GOP

Group of pictures: individual frames grouped together, forming a video-motion sequence.

Grace period

When you install your system, configure it and add recording servers and cameras, your system runs on temporary licenses. These need to be activated before a certain period ends. This is the grace period.

GUID

Globally unique identifier—unique 128-bit number used to identify components on a Windows system.

H

H.264

A standard for compressing and decompressing video data (a codec). H.264 is a codec that compresses video more effectively than older codecs, and it provides more flexibility for use in a variety of network environments.

Hardware device

When you add a digital camera to your system, you are not adding the camera itself only, but rather hardware devices. Hardware devices have their own IP addresses or host names. Being IP-based, your system primarily identifies units based on their IP addresses or host names.

Even though each hardware device has its own IP address or host name, you can attach several cameras, microphones and speakers to a single hardware device and share the same IP address or host name. This is typically the case with cameras attached to video encoder devices.

You can configure each camera, microphone and similar channels on the hardware device individually, even when several of them are attached to a single hardware device.

Host

A computer connected to a TCP/IP network. A host has its own IP address, but may—depending on network configuration—also have a **host name to make it easily identifiable.**

Hotspot

Particular position for viewing enlarged and/or high quality video in the Smart Client.

I

I/O

Input/Output: refers to the communication between a computer and a person. Inputs are the signals or data received by the system and outputs are the signals or data sent from it.

I-frame

Short name for intra-frame. Used in the MPEG standard for digital video compression. An I-frame is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files. An I-frame is similar to a keyframe.

Image Server

A service that handles access to XProtect Professional for remote users logging in with Smart Client The Image Server service does not require separate hardware as it runs in the background on the XProtect Professional server. The Image Server service is not configured separately as it is configured through XProtect Professional 's Management Application.

IPIX

A technology that allows the creation and viewing of 360-degree panomorph (fisheye) images.

J

JPEG

(Also JPG) Joint Photographic Experts Group—widely used lossy compression technique for images.

K

Keyframe

Used in the MPEG standard for digital video compression, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the frames between the keyframes record only the pixels that change. This helps greatly reduce the size of MPEG files.

M

MAC address

Media Access Control address—12-character hexadecimal number uniquely identifying each device on a network.

Manual events

You can generate an event manually from the client. These events are called manual events.

Master/Slave

A setup of servers where one server (the master server) is of higher importance than the remaining servers (the slave servers). With a master/slave setup in your system, you can combine several XProtect Professional servers and extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server. In such a setup, clients still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers.

Matrix

A feature that enables the control of live camera views on remote computers for distributed viewing. Once configured, you can view Matrix-triggered live video in XProtect Smart Client.

Matrix recipient

A computer equipped with XProtect Smart Client software and therefore capable of displaying Matrix-triggered live video.

MJPEG

Motion JPEG—compressed video format where each frame is a separately compressed JPEG image. The method used is quite similar to the I-frame method used for MPEG, but no interframe prediction is used. This allows for somewhat easier editing, and makes compression independent of the amount of motion.

Monitor

1) A computer screen. 2) An application used in previous versions of XProtect Professional for recording and displaying video. The Monitor application has been discontinued.

MPEG

Compression standards and file formats for digital video developed by the Moving Pictures Experts Group. MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information. Keyframes stored at specified intervals record the entire view of the camera, whereas the frames that follow record only pixels that change. This helps greatly reduce the size of MPEG files.

N

NTLM

In a Windows network, NT LAN Manager is a network authentication protocol.

P

Panomorph

A type of lens that allows the creation and viewing of 360-degree images.

P-frame

Predictive frame—the MPEG standard for digital video compression uses P-frames

together with I-frames. An I-frame, also known as a keyframe, is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (the P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files.

PIN

Personal identification number (or personal identity number)—number used to identify and authenticate users.

Ping

A computer network administration utility used to determine whether an IP address is available, by sending a small amount of data to see if it responds. The word ping was chosen because it mirrors the sound of a sonar. You send the ping command using a Windows command prompt.

Polling

Regularly checking the state of something, for example, whether input has been received on a particular input port of a device. The defined interval between such state checks is often called a polling frequency.

Port

Logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic, which is used when viewing web pages.

POS

(Also PoS) Point of sale: the physical place where a sale is made, for example, at the cash register.

Post-recording

The ability to store recordings from periods following motion and/or specified events. Based on incoming video being buffered on the XProtect Professional server in case it is going to be needed for a motion- or event-triggered recording. Using post-recording can be highly advantageous: if, for example, you have defined that video should be recorded while a gate is open, being able to see what happens immediately after the gate is closed may also be important.

Pre-alarm

Pre-alarm images is a feature available for selected cameras only. It enables the sending of images from immediately before an event took place from the camera to XProtect Professional via e-mail.

Pre-buffer

See the description of Pre-recording.

Pre-recording

The ability to store recordings from periods preceding detected motion and/or specified events. Based on incoming video being buffered on the XProtect Professional server in case it is going to be needed for a motion- or event-triggered recording. Using pre-recording can be highly advantageous: if, for example, you have defined that video should be recorded when a door is opened, being able to see what happened immediately prior to the door being opened may also be important.

Privacy masking

The ability to define if and how selected areas of a camera's view should be masked before distribution. For example, if an XProtect Professional camera films a street, you can mask certain areas of a building (for example, windows and doors) with privacy masking in order to protect residents' privacy.

PTZ

Pan-tilt-zoom. A highly movable and flexible type of camera.

PUK

Personal Unblocking Key or PIN Unlock Key—number used as an extra security measure for SIM cards.

R

Recording

On IP video surveillance systems, recording means **saving video and, if applicable, audio from a camera in the cameraâ€™s database on the surveillance system**. In many IP surveillance systems, all the video/audio received from cameras is not necessarily saved. Saving of video and audio in a cameraâ€™s database is in many cases started only when there is a reason to do so, for example, when motion is detected, when an event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, for example, when motion is no longer detected, when an event occurs, or when a time period ends. The term **recording** originates from the analog video era, when images were taped only when the record button was pressed.

Recording Server service

Windows service (without any user interface) used by your system for recording and displaying video. Video is only transferred to the surveillance system while the Recording Server service is running.

Restore point

Restore points allow you to return to a previous configuration state. When a configuration change is applied in XProtect Professional, a restore point is created. If something goes wrong in your configuration, you can browse through restore points, and return to a suitable one.

S

SCS

A file extension (.scs) for a script type targeted at controlling clients.

SDK

Software Development Kit—programming package enabling software developers to create applications for use with a specific platform.

SIM

Subscriber identity module—circuit stored on a small card inserted into a mobile phone or computer, or other mobile device. The SIM card is used to identify and authenticate the user.

SLC

Software license code—product registration code required for using the XProtect Professional software. If you do not have system administration responsibilities, you do not have to deal with SLCs. System administrators use SLCs when installing and registering the software.

SMTP

Simple Mail Transfer Protocol—standard for sending e-mail messages between mail servers.

Subnet

A part of a network. Dividing a network into subnets can be advantageous for management and security reasons, and may in some cases also help improve performance. On TCP/IP-based networks, a subnet is basically a part of a network on which all devices share the same prefix in their IP addresses, for example 123.123.123.xxx, where the first three numbers (123.123.123) are the shared prefix. Network administrators use subnet masks to divide networks into subnets.

T

TCP

Transmission Control Protocol—protocol (or standard) used for sending data packets across networks. TCP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

TCP/IP

Transmission Control Protocol/Internet Protocol—combination of protocols (or standards) used when connecting computers and other devices on networks, including the internet.

Telnet

Terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet.

Transact

An add-on to your XProtect VMS system. XProtect Transact can help you prevent loss and shrinkage through video evidence combined with time-linked POS or ATM transaction data.

U

UDP

User Datagram Protocol—connectionless protocol for sending data packets across networks. Primarily used for broadcasting messages. UDP is a fairly simple protocol, with less error recovery features than, for example, the TCP protocol.

UPS

A UPS (Uninterruptible Power Supply) works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

V

VCA

Video content analysis (VCA) is a system that detects various types of previously specified behavior, both of humans and vehicles. A VCA-based system provides third-party video content analysis, spanning from face recognition, over advanced motion detection, to complex behavioral analysis. VCA systems and their output can seamlessly be integrated with the **Alarms** feature and used for, for example, triggering alarms. Here, the events resulting from VCA systems are called analytics events.

Third-party VCA tools are developed by independent partners delivering solutions based on an a Milestone open platform. These solutions can impact performance on XProtect Professional.

Video encoder

A device, typically a standalone device, that can stream video from a number of connected client cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

Video server

Another name for a video encoder.

View

In XProtect Professional, a collection of video from one or more cameras, presented together in the Smart Client. A view may include other

content, such as HTML pages and static images, in addition to video from cameras.

VMD

Video motion detection. A way of defining activity in a scene by analyzing image data and the differences in a series of images.

W

Wizard

A utility to help perform a particular task quickly, while also ensuring coverage of all relevant parameters. For example, the **Adjust Motion Detection** wizard quickly helps you configure motion detection on each of XProtect Professional's cameras without the risk of forgetting to set any key parameters.

Index

3

360 degrees panomorph support • 204

360° lens • 100

A

About access control integration • 153

About accessing logs and exports • 181, 182

About administrator rights • 10

About alarms • 184, 186

About archiving • 47, 49, 50, 51, 52, 53, 66, 73, 74, 76, 86, 94, 128, 136, 194

About archiving audio • 130

About archiving locations • 129

About archiving schedules • 131

About archiving to other locations • 129

About automatic device discovery • 191, 192

About back up and restore of configuration • 197

About Central • 152

About database resizing • 66

About daylight saving time • 11

About dedicated input/output devices • 59, 117

About direct streaming • 173

About dynamic archive paths • 129

About email • 146

About events and output • 109

About hardware devices • 58

About important port numbers • 10

About input and output • 109

About licenses • 25

About logs • 141

About maps • 185

About master and slave • 164

About Matrix video sharing • 35, 138

About Matrix-recipients • 138

About microphones • 58, 107

About Milestone Mobile client • 18

About minimum system requirements • 10

About MIP plug-ins • 190

About Mobile server • 173

About Mobile Server Manager • 20, 181

About motion detection • 66, 70, 97

About motion detection and PTZ cameras • 68, 70

About notifications • 113, 146

About protecting recording databases from corruption • 35, 95

About recording audio • 58

About registered services • 162

About removing system components • 32

About replacing cameras • 26

About replacing hardware devices • 60

About restarting services • 38

About saving changes to the configuration • 36

About saving configuration changes in XProtect Enterprise 8.1 and streamlined software versions • 174

About scheduling • 127

About scheduling of notifications • 151

About seeing license information • 26

About server access • 161

About services • 66, 172

About show status • 182

About SMS • 149

About speakers • 58

About the Getting started page • 40

About the Replace Hardware Device wizard • 27, 60, 61, 64

About time servers • 11

About updates • 31

About upgrading • 30

About upgrading from one current XProtect Professional VMS product to another current XProtect Professional VMS product • 32

About upgrading from one product version to another product version • 31

About users • 166

About using the built-in help • 37

About video and recording configuration • 34, 63, 65, 68, 72, 74, 80, 81, 84, 85, 86, 88, 89, 91, 92, 93, 96, 97, 101, 108, 137

About Video push • 174

About viewing archived recordings • 133

About virus scanning • 12, 133

About XProtect Smart Client • 16

About XProtect Web Client • 20

Access control • 153

Access Control Actions • 158

Access Control Events tab (Access Control) • 157

Access control management • 171

Access control properties • 155

Access XProtect Web Client • 20, 181

Add a generic event • 111, 113

Add a hardware input event • 111, 120

Add a hardware output • 96, 109, 111, 112, 114, 121

Add a manual event • 111, 113, 121, 187

Add a time profile (for alarms) • 185, 186, 187, 190

Add a timer event • 111, 112, 113, 114, 121, 122, 127

Add a Video push channel • 174, 175, 178

Add a Video push driver as a hardware device • 174, 175

Add an alarm • 186, 187

Add an analytics event • 111, 118

Add basic users • 35, 166, 167, 168, 169, 171

Add hardware

Import from CSV file - CSV file format and requirements • 44

Scanning options • 42

Select hardware manufacturers to scan for • 43

Add hardware devices settings • 175

Add Hardware Devices wizard - Import from CSV File - example of CSV file • 44

Add hardware wizard • 41, 58

Add user groups • 35, 56, 167, 168, 169, 171

Add Windows users • 166, 167, 168, 169, 171

Add/edit a Mobile server • 174

Adjust motion detection

Exclude regions • 54, 70

Motion detection • 54

Adjust motion detection wizard • 53

Administrator • 204

Advanced configuration • 58

Alarm data settings • 188

Alarm management • 171

Alarms • 184

Alarms definition • 115, 186, 187, 188, 189

Alarms properties • 187

Analytics event • 111, 118

Analytics Event Settings • 194

Analytics Events • 204

API • 204

Archiving • 131, 133, 136

Aspect ratio • 204

Associated cameras • 154

Associated Cameras tab (Access Control) • 156

ATM • 204

Attachment Settings (email) • 147

Audio • 91

Audio recording • 85

Audio selection • 86

Auto Export Rule window settings • 179

Automatic configuration wizard • 34, 40

Continue after scan • 41

First page • 40

Scanning for hardware devices • 41

Scanning options • 40

Select hardware manufacturers to scan for • 40

Automatic response if running out of disk space • 131

AVI • 204

B

Back up and restore alarm and map configuration • 198

Back up and restore configuration • 197

Back up system configuration • 31, 197

Before you start • 10

Best practices • 35

C

Camera access • 135, 167, 168, 169

Camera and database action • 62

Camera properties • 88

Cameras and storage information • 65

Camera-specific scheduling properties • 136

Cardholders tab (Access Control) • 160

Carousel • 204

Central • 152, 204

Central properties • 152

Change default file paths • 191

Clients • 16

Codec • 204

Configure camera-specific schedules • 35, 68, 70, 134, 136, 137, 138

Configure email notifications • 120, 122, 126, 146

Configure general event handling • 111, 115, 116, 123

Configure general scheduling and archiving • 35, 70, 133, 135

Configure hardware devices • 60, 63, 64, 101

Configure hardware output on event • 109, 111, 112, 113, 114, 127

Configure master and slave servers • 35, 164

Configure Matrix • 139

Configure microphones or speakers • 107

Configure motion detection • 70

Configure server access • 35, 56, 162

Configure SMS notifications • 149

Configure storage

- Drive selection • 50
- Live and recording settings (motion JPEG cameras) • 47
- Live and recording settings (MPEG cameras) • 48
- Online schedule • 46
- Recording and archiving settings • 52
- Video settings and preview • 45

Configure storage wizard • 45, 129, 131

Configure system, event and audit logging • 144

Configure user and group rights • 35, 56, 57, 96, 102, 113, 167, 168

Configure when cameras should do what • 70

Connecting to the access control system • 154

Copyright, trademarks and disclaimer • 9

Create access control system integration • 154

CSV • 204

D

Default File Paths • 129, 194, 197

Delete hardware devices • 60, 71

Device • 204

DirectX • 205

Disable information collection • 191

Disable or delete cameras • 70

DNS • 205

Driver • 205

DST • 205

Dual stream • 205

DVR • 205

Dynamic path selection (properties) • 66, 74, 95, 194

E

Edit certificate • 181, 182

Email • 146

Email (Properties) • 136, 146

Enable XProtect Central • 152

Event notification • 96

Event Server • 205

Event Server Settings • 195

Events and output • 109

Events and output properties • 118

Export • 178

Export and import management application configuration • 197, 201

Express • 41, 42

F

Fill in/edit surveillance server credentials • 181, 183

Final summary • 155

First time use • 34

Fisheye • 60, 100, 101, 205

FPS • 205

Frame rate • 205

Frame rate - MJPEG • 81, 137

Frame Rate - MPEG • 84

G

General • 49, 76, 88, 92, 97, 176, 192

General access • 167, 168, 169, 171

General event properties • 117

General scheduling properties • 133

General Settings tab (Access Control) • 155

Generate alarms based on analytics events • 115

Generic event • 123

Generic events • 205

Get your system up and running • 28, 34, 200

Getting started • 40

GOP • 205

Grace period • 205

Group information • 168

GUID • 206

H

H.264 • 206

Hardware detection and verification • 43

Hardware device • 206

Hardware devices • 58

Hardware input event • 112, 113, 120

Hardware name and video channels • 63

Hardware output • 121

Hardware properties • 63

Host • 206

Hotspot • 206

I

I/O • 206

If the camera uses the MJPEG video format • 77

If the camera uses the MPEG video format • 79

I-frame • 206

Image Server • 206

Import changes to configuration • 202

Import from CSV file • 42, 43, 44

Information, driver selection and verification • 43

Install and upgrade • 28

Install from the management server • 17

Install Milestone Mobile client • 19

Install silently • 17, 28

Install video device drivers • 30

Install XProtect Smart Client • 17

Install your system software • 28, 34, 186

IPIX • 206

J

JPEG • 206

K

Keyframe • 207

L

Language support and XML encoding • 164

Licenses • 25

Local IP ranges • 163

Log properties • 144

Log Settings • 181

Logs • 141

M

MAC address • 207

Manage user access

Access summary • 57

Basic and Windows users • 56

Manage user access wizard • 35, 56, 168

Manual • 42, 43

Manual event • 121

Manual events • 207

Manual recording • 80, 93, 170

Master/Slave • 164, 207

Master/slave properties • 164

Matrix • 138, 207

Matrix event control • 139, 140

Matrix properties • 139

Matrix recipient • 207

Matrix recipients • 139

Message Settings (email) • 146, 151

Message Settings (SMS) • 149, 151

Microphone (properties) • 108

Microphones • 107

Milestone Mobile client • 18

MIP plug-ins • 190

MJPEG • 207

Mobile server • 173

Mobile Server Manager • 181

Mobile server settings • 176

Monitor • 207

Monitor storage space usage • 38

Motion detection & exclude regions • 49, 70, 76, 83, 85, 92, 97, 112

Move PTZ type 1 and 3 to required positions • 71

MPEG • 207

N

Network, device type, and license • 60, 63

New hardware device information • 61

Notification Scheduling properties • 147, 150, 151

Notifications • 146

NTLM • 207

O

Online period • 49, 70, 76, 88, 92, 113, 135, 136

Options • 192

Output • 96, 112

Output control on event (Events and Output-specific properties) • 114, 127

Overview of events and output • 109

P

Panomorph • 207

Performance • 179

P-frame • 208

PIN • 208

Ping • 208

Polling • 208

Port • 208

Ports and polling • 59, 115, 117

POS • 208

Post-recording • 208

Pre-alarm • 208

Pre-buffer • 208

Pre-recording • 208

Privacy masking • 99, 208

PTZ • 209

PTZ device (properties) • 60, 64

PTZ on event • 106, 113

PTZ patrolling • 68, 104, 135, 137, 138

PTZ preset positions • 102, 106

PUK • 209

R

Recording • 75, 80, 81, 84, 92, 120, 172, 209

Recording and archiving paths • 93, 194

Recording and archiving paths (properties) • 72

Recording and storage properties • 72

Recording Server Manager • 21

Recording Server service • 209

Regular frame rate properties • 82

Restore point • 209

Restore system configuration • 198

Restore system configuration from a restore point • 37, 203

S

Scheduling • 151

Scheduling all cameras • 133

Scheduling and archiving • 127

Scheduling options • 46, 133, 135, 136, 137

SCS • 209

SDK • 209

Server access • 11, 161, 162

Server access properties • 162

Server Settings (email) • 148

Server Settings (SMS) • 150

Server Status • 176

Servers • 173

Services • 172

Settings • 191

Show or hide microphones or speakers • 59, 108

Show/edit port numbers • 181, 183

SIM • 209

SLC • 209

SMS • 149

SMS properties • 149

SMTP • 209

Sound settings • 188, 189

Speaker properties • 63, 108

Speedup • 79, 83, 85, 137

Speedup frame rate properties • 82

Start and stop services • 39, 53, 54, 60, 97, 103, 104, 107, 172, 173

Start, stop and restart Mobile service • 181, 183

Storage capacity required for archiving • 130

Storage information • 87

Subnet • 209

System maintenance • 197

System overview • 14

T

TCP • 210

TCP/IP • 210

Telnet • 210

Template and common properties • 81

Test a generic event • 115, 123

Time profile • 190

Timer event • 114, 122

Transact • 210

U

UDP • 210

Upgrade • 30

Upgrading from one current XProtect Professional VMS product to another current XProtect Professional VMS product • 32

Upgrading from one product version to another product version • 28, 31, 34, 197

UPS • 36, 210

User information • 168

User Interface • 193

User properties • 168

Users • 166

V

VCA • 115, 210

Video • 84, 89, 137

Video encoder • 210

Video Push • 175, 177

Video recording (properties) • 74

Video server • 211

View • 211

View video from cameras in Management Application • 39, 53, 54, 97, 103, 104, 107

VMD • 211

W

Wizard • 211

Wizard for access control system integration • 153

X

XProtect Download Manager • 22

XProtect Smart Client • 16

XProtect Web Client • 20

About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit:

www.milestonesys.com.